Қолданылған әдебиеттер тізімі

1. Скрипчинский А.В., Антонов С.А. Космический Мониторинг Пастбищ Восточных Районов Ставропольского Края // Наука. Инновациию Технологии, №2, 2019, С. 125-134.
2. E. Nkonya , A. Mirzabaev , Economics of Land Degradation and Improvement – A Global Assessment for Sustanaible Development // Bonn: Springer; 2016. 685 p.
3. S. Vasilyev Irrigatedagrolandscape monitoring taking into account remote sensing data calibration under geoinfromation technologies // Научный журнал КубГАУ, №131(07), 2017.
4. G. Andreas Радиометрическая коррекция VNIR данных ASTER; [Электрон. Ресурс.] - 2018 -URL: https://gis-lab.info/qa/aster_radiocorr.html (дата обращения:23.03.2020).
5. A.Soloviev, J. Zharkikh, R. Krasnoperov, B. Nikolov, S. Agayan GIS-oriented solutions for advanced clustering analysis of geoscience data using ArcGIS platform // RUSSIAN JOURNAL OF EARTH SCIENCES, VOL. 16, ES6004, doi:10.2205/2016ES000587, 2016.
6. Ольшевский А., Самсоненков И., Яцухно М. Технология выявления, дешифрирования и картографирования деградированных земель на основе данных дистанционного зондирования Земли // Журнал Белорусского государственного университета, №2, 2018. С.50 – 58.
7. A. Bychkov, USING OF GEOINFORMATIONAL SYSTEM FOR SOLVING APPLIED TASKS [Электрон. Ресурс.] // -2017-URL: https://ipi1.ru/s/05-00-00-tekhnicheskie-nauki/1798-ispolzovanie-geoinformatsionnykh.html (дата обращения:23.03.2020).

ОӘЖ 004.771

MICROSOFT AZURE БҰЛТЫНЫҢ ЖЕЛІЛІК ҚАУІПСІЗДІГІ. ҚАУІПСІЗДІК ОПЕРАЦИЯЛАРЫ

Бегатай Улжалғас Бақтыбайқызы

Ulzhalgas.Begatay@mail.ru

Л. Н. Гумилев атындағы Евразия ұлттық университетінің 2-курс магистранты,

Нұр-Сұлтан, Қазақстан

Ғылыми жетекші – Информатика және ақпараттық қауіпсіздік кафедрасының доценті, ф.-м. ғ. к. Сексенбаева А.К.

Аннотация: Ақпарат—бүгінгі қоғамның дамуындағы басты ресурс. Қазірде барлық ақпараттарымыз электронды сақталады, хабарламалар желіліер арқылы жіберіледі, сондықтанд да желі қауіпсіздігінің маңызы өті зор. Мақала Microsoft Azure бұлтының желілік қауіпсіздігі және қауіпсіздік операциялар туралы жазылды.

Кілттік сөздер*:* желілік қауіпсіздік, зиянды бағдарламалар, инцидент.

Желілік қауіпсіздік - кәсіпорынның қауіпсіздігін қамтамасыз етудің негізгі тірегі. Алайда бұлтты есептеулер желі периметрлеріне анағұрлым қауіпке төтеп беру талабын жоғарылатты және көптеген қасақана әрекет жасаушылар идентификация жүйесінің элементтеріне шабуыл жасау өнерін игерді (олар желіні басқаруды әрдайым дерлік айналып кетеді). Бұл факторлар желі негізінде қол жетімділікті басқару элементтеріне емес, ресурстарды қорғау үшін сәйкестендіру негізінде қол жетімділікті басқару элементтеріне шоғырлану қажеттілігін арттырды.

Көптеген қасақана әрекет етушілер бұрынғысынша сканерлеу және желі қауіпсіздігінің базалық ережелерін сақтамайтындар үшін қорғауға ойдағыдай еніп, жалпы қол жетімді бұлттар провайдерлерінің IP-адрестерінің диапазондарында пайдалану әдістерін пайдаланады. Желілік қауіпсіздікті басқару құралдары, сондай-ақ бұлттық өрістетулерге түсетін қарсы әрекеттерді қорғауға, анықтауға, тежеуге және тастауға көмектесетін қорғаныс стратегиясының элементін қамтамасыз етеді.

Желілік қауіпсіздік және қорғау санатында келесі сипаттамалар бар:

- ✓ Желілік сегментацияны жалпы стратегиямен біріктіру;
- ✓ Орталықтандырылған желіні басқару және қауіпсіздік;

- ✓ Желіні тежеу стратегиясын жасау;
- ✓ Интернет стратегиясын анықтау.

Орталықтандырылған желіні басқару және қауіпсіздік

Виртуалды желілердің, кіші желілердің және IP-адрестердің схемалары, сондай-ақ виртуалды желілік құрылғылар, бұлттағы виртуалды желінің белсенділігін шифрлеу және үйаралық қызмет сияқты желілік қауіпсіздік элементтері сияқты негізгі желілік функциялардың қауіпсіздігі мен басқаруына ұйымдастырушылық жауапкершілікті орталықтандыру.

Біз желіні басқару мен қауіпсіздікті орталықтандырған кезде, қауіпсіздік тәуекелдерін пайдалану үшін ықтимал қаскүнем құруы мүмкін үйлеспейтін стратегиялардың ықтималдығын азайтамыз.

Желілік сегментацияны жалпы стратегиямен біріктіру;

Ұйымның желіні сегменттеу моделімен жалпы сегменттеу модельмен үйлестіру.

Бұл түсінбестікті және әр түрлі техникалық топтармен (желілермен, сәйкестендірумен, қосымшалармен және т.б.) туындайтын проблемаларды азайтады, олардың әрқайсысы бір-біріне сәйкес келмейтін өз сегменттеу мен делегациялаудың модельдерін әзірлейді. Бұл қарапайым және біріздендірілген қауіпсіздік стратегиясына алып келеді, ол адам қателігінен қателер санын азайтуға және автоматтандыру есебінен сенімділікті арттыруға мүмкіндік бермеуіне көмектеседі.

Қауіпсіздік сақтау стратегиясын жасау

Тәуекелді болдырмау стратегиясын дәлелденген тәсілдер арқылы жасау, соның ішінде:

Желі қауіпсіздігін бақылау және тәжірибе құралдары;

Қауіпсіздікті басқару құралдары Azure -да қол жетімді;

Нөлдік сенім тәсілдері.

Интернет стратегиясын анықтау

Интернет шекарасында қауіпсіздікті қамтамасыз ету үшін бұлт провайдері немесе виртуалды желі құрылғысының жеке басқару элементтерін пайдалану мүмкіндігін таңдау.

Интернет шекарасында қауіпсіздікті бақылау мен мониторингілеуді қамтамасыз ететін екі негізгі нұсқасы бар:

Бұлт провайдерін басқару элементтері (Azure брандмауэр + веб-қосымшалар брандмауэр (WAF))

Серіктестер үшін виртуалды желілік құрылғылар (брандмауэр және WAF жабдықтаушылары Azure Marketplace)

Бұлттық қызмет провайдерінің жеке басқару элементтері әдетте OWASP Top 10 сияқты кең таралған шабуылдар үшін жеткілікті жақсы базалық қорғауды ұсынады.

Керісінше, бұлт қызметтері провайдерінің мүмкіндіктері көбінесе шабуылдардан қорғай алатын анағұрлым озық функцияларды ұсынады. Серіктестік шешімдер кірістірілген басқару құралдарына қарағанда өзгеріссіз қымбат. Сонымен қатар, серіктестік шешімдер конфигурациясы өз басқару элементтеріне қарағанда өте күрделі және нәзік болуы мүмкін, себебі олар бұлт фабрикасының бақылаушыларымен біріктірілмейді.

Қауіпсіздік операциялары жүйенің қауіпсіздік кепілдігін қолдайды және қалпына келтіреді. Қауіпсіздік міндеттері NIST Cybersecurity Framework функцияларында жақсы сипатталған: анықтау, жауап беру және қалпына келтіру.

Анықтау - қауіпсіздік операциялары көптеген жағдайларда жасырын қалуға ұмтылатын жүйеде қарсы жақтардың болуын анықтау керек, себебі бұл оларға өз мақсаттарына кедергісіз қол жеткізуге мүмкіндік береді. Бұл кәсіпорын белсенділігінің журналдарында күдікті белсенділік немесе жалпы заңдылықтан ауытқыған оқиғалар туралы ескерту әрекет ету нысанын қабылдауы мүмкін.

Жауап - қарсы жақтың ықтимал әрекеті анықталған кезде қауіпсіздікті қамтамасыз ету жөніндегі операциялар, бұл нақты шабуыл (шынайы оң) немесе жалған дабыл (жалған оң) болып табылатынын анықтау үшін, содан кейін қарсы жақтың операцияның көлемі мен мақсатын көрсету үшін тергеу тез жүргізілуге тиіс.

Қалпына келтіру - қауіпсіздікті қамтамасыз ету жөніндегі операциялардың соңғы мақсаты-шабуыл кезінде және одан кейін бизнес-сервистердің қауіпсіздік кепілдігін (құпиялылығын, тұтастығын, қол жетімділігін) сақтау немесе қалпына келтіру.

Көптеген ұйымдар тап болатын қауіпсіздік үшін едәуір тәуекел адамдардың шабуылына (түрлі біліктілік деңгейіне) байланысты. Бұл зиянды бағдарламалардан қорғауға орнатылған сигналдар мен машиналық оқытуға негізделген тәсілдердің арқасында көптеген ұйымдар үшін автоматты немесе қайталанатын шабуылдардан тәуекел айтарлықтай төмендеуімен байланысты (дегенмен қорғаныстардан тезірек қозғалатын Wannacrypt (Microsoft Windows операциялық жүйесінің басқаруындағы компьютерлерді ғана зақымдайтын ақша қаражатын бопсалаушы бағдарлама. Компьютерді жұқтырғаннан кейін құрт бағдарламалық коды компьютерде сақталған барлық файлдарды шифрлайды және криптовалютта ақша құнын төлеуді ұсынады. Зақымданған сәттен бастап 7 күн ішінде сатып алу төленбеген жағдайда, файлдарды шифрлеу мүмкіндігі мәңгілікке жоғалады.) және NotPetya (Microsoft Windows басқаруындағы компьютерлерді зақымдайтын зиянды бағдарлама. Вирустың алғашқы түрлері 2016 жылдың наурызында анықталды)).

Қауіпсіздік операциялары (кейде қауіпсіздік операцияларының орталығы (SOC) деп аталатын) қастық ойлаушының уақытын және бағалы жүйелер мен деректерге қол жеткізуін шектеуде маңызды рөл атқарады. Қастық ойлаушының ортасында бар әрбір минут оларға шабуыл операцияларын жүргізуді жалғастыруға және сезімтал / бағалы жүйелерге қол жеткізуге мүмкіндік береді.

Мақсаты мен метрикасы

Сіз өлшеп отырған көрсеткіштер қауіпсіздікті қамтамасыз ету бойынша іс-әрекеттер мен нәтижелерге елеулі әсер етеді. Дұрыс өлшемдерге назар аудару тәуекелді айтарлықтай төмендететін дұрыс салаларда үздіксіз жақсартуды қамтамасыз етуге көмектеседі.

Қауіпсіздік операциялары қастық ойлаушылардың кіруін тиімді шектейтініне кепілдік беру үшін мақсаттар

Қорғаушылардың жалған жұмыс істеуді тергеуге уақыт жұмсағанына дейін табылған қарсыластар елемейді көз жеткізу үшін ескертуді растау үшін уақытты қысқарту.

Табылған зиянкестерді түзету үшін уақытты қысқарту, оларды жүргізу мен шабуылға және сезімтал жүйелерге қол жеткізу уақытын қысқарту.

Жоғары ішкі құндылығы бар (ықтимал мақсаттар / бизнеске үлкен әсер ету) және көптеген жүйелерге немесе сезімтал жүйелерге (әкімшілердің есептік жазбалары және құпия пайдаланушылар) қол жеткізе алатын жүйелердегі қауіпсіздікке инвестицияларды приоритизациялау)

Кәсіпорынның гибридті түрі

Қауіпсіздік операциялары олардың құрал-саймандары, процестері мен талдаушылар дағдыларының жиынтығы олардың гибридті жай-күйінің барлық диапазонында көрінуді қамтамасыз ететініне кепілдік беруі тиіс.

Қасақана әрекет етуші ұйымға бағытталған кезде белгілі бір ортамен өз іс-әрекеттерін шектемейді, олар кез келген платформада кез келген қолжетімді тәсілмен ресурстарға шабуыл жасайды. Azure және AWS сияқты бұлтты сервистерді енгізетін корпоративтік ұйымдар бұлтты және жергілікті активтердің будандарын тиімді пайдаланады.

Қауіпсіздікті қамтамасыз ету жөніндегі операциялардың құралдары мен процестері бұлтты және жергілікті активтерге шабуыл жасау үшін, сондай-ақ куәліктерді немесе басқа да құралдарды пайдалана отырып, бұлтты және жергілікті ресурстар арасында бұрылатын шабуылшыларға арналған болуы тиіс. Бұл жалпы ұйымдастыру көрінісі жедел қауіпсіздік топтарына шабуылдарды тез анықтауға, оларға әрекет етуге және ұйымдастыру тәуекелдерін төмендетіп, қалпына келтіруге мүмкіндік береді.

Жеке табулар мен басқару элементтерін пайдалану.

Бұлттан оқиғалар журналдарын пайдалану арқылы пайдаланушы табуларды жасау алдында бұлт платформасына орнатылған қауіпсіздік пен басқару құралдарын пайдалануға артықшылық беру керек.

Бұлт платформалары анықтауды қиындататын жаңа функциялардың арқасында тез дамиды. Бұлт қызметі провайдері өз бақылауын қолдайды және әдетте жоғары сапалы (төмен жалған жұмыс).

Көптеген ұйымдар бірнеше бұлт платформаларын пайдалана алады және барлық кәсіпорын бойынша бірыңғай көріністі қажет ететіндіктен, бұл меншікті табулар мен басқару элементтері орталықтандырылған SIEM немесе басқа құралмен қамтамасыз етілетініне көз жеткізу керек. Біз өз табулары мен басқару элементтерінің орнына сұраулар мен сұраныстарды талдаудың жалпылама құралдарын ауыстыруға тырыспауға кеңес бермейді. Бұл құралдар белсенді аңшылық қызметі үшін көптеген артықшылықтарды ұсына алады, бірақ осы құралдардың көмегімен жоғары сапалы хабардар ету үшін аң аулау мен басқа да қызмет түрлерін жұмсауға болатын терең тәжірибе мен уақытты талап етеді.

Орталықтандырылған SIEM кең көрінуін толықтыру үшін (Azure Sentinel, Splunk немесе QRadar сияқты), өз табыстарын және басқару элементтерін пайдалану керек.

Azure пайдаланатын ұйымдар Azure платформасында ескерту жасау үшін Azure Security Center сияқты мүмкіндіктерді пайдалануы тиіс.

Ұйымдар Azure Monitor және AWS CloudTrail сияқты журналдарды орталықтандырылған көрініске шығару үшін өз мүмкіндіктерін пайдалануы тиіс.

Azure пайдаланатын ұйымдар Azure платформасында желілік операцияларды қарау үшін Network Security Group (NSG) мүмкіндіктерін пайдалануы тиіс.

Тексеру әдістері соңғы нүктелерді анықтау және ден қою шешімі (EDR), сәйкестендіру құралдары және Azure Sentinel сияқты активтердің түрі туралы терең білімі бар жеке құралдарды пайдалануға тиіс.

Хабарландыру басымдығы және журнал интеграциясы

Көз жеткізіңіз интегрируете сыни алдын алу қауіпсіздігі және sen в SIEM емес енгізе отырып, мәліметтердің үлкен көлемін төменгі маңызы бар.

Жиналатын деректер осы операциялардың біреуін немесе бірнешеуін қолдауға бағытталуы тиіс:

Жариялау (қолда бар құралдардан табу немесе пайдаланушылық жариялануды жасау үшін қажетті деректер);

Инцидентті тексеру;

Профилактикалық іс-шаралар.

Көп деректердің интеграциясы тез реакцияны және түзетуді қамтамасыз ететін (жалған іске қосылуларды сүзу, шынайы оң нәтижелерді арттыру және т.б.) қосымша контекстпен хабарлауды байытуға мүмкіндік береді, бірақ деректерді жинау анықтамайды. Егер сізде деректер құндылыққа ие болады деген ой жоқ болса (мысалы, брандмауэрдің үлкен көлемі оқиғаға тыйым салады), сіз осы оқиғаларды интеграциялау басымдығын жоя аласыз.

Қолданылған әдебиеттер тізімі

1. http://azure.microsoft.com
2. https://www.ptsecurity.com
3. Юрий Диогенес и д-р Томас В. Шиндер. Инфраструктура безопасности Microsoft Azure. 2016. С.4-7

УДК 004

ПРИМЕНЕНИЕ СИСТЕМЫ КОМПЛЕКСНОЙ АВТОМАТИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ WEBTUTOR В ДИСТАНЦИОННОМ ОБУЧЕНИИ

Берденкулов Е., Ахметова Ж.Ж.
berdenkulov@mail.ru
Магистрант 2-курса Финансовой Академии