ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

Веб-қосымшаның пентест кезеңінде маңызды осалдықтары табылды. Осалдықтар веб-қосымшаны толықтай бұзуға, яғни, деректердің құпиялылығының толық бұзылуына, ұрлынуына, жоғалуына мүмкіндік береді.

Қортынды

Интернет-ресурстардың өмірімізге біртіндеп енгізілуі қызметтер мен кеңес алуда үлкен артықшылықтарды береді. Веб-қосымшалардың функционалдық дамуы қауіпсіздікті сапалы қамтамасыз етумен қатар жүруі тиіс. Қосымшалардың қауіпсіздігін қамтамасыз етуде қауіп төндіретін мәліметтер жиынтығынан тұратын базалардың маңызы зор. Пентест зиянкестердің әрекеттерін толығымен модельдеуге және ресурстардың қауіпсіздігін сапалы бағалауға мүмкіндік беретін әдістердің бірі. Пентест бойынша жұмыстарды жүргізу үшін тестілеуге қажет құралдар мен әдістемелер зерделенді.

Баяндалған ақпаратты қорытындылай келе, веб-қосымшаны қорғау үшін келесі жалпы іс-шараларды өткізу ұсынылады:

- Жаңартуларды уақытында орнатып отыру
- Парольдерді дұрыс орында сақтау;
- Керек емес порттарды жабу;
- Брэнмаур жүйесін қосу;
- Қолданылмайтын қосымша әдістерді алып тастау;
- Дерекқор пайдаланушысының құқықтарын шектеу;
- Қызметтік файлдарға тікелей кіруге тыйым салу.

Пайдаланылған дереккөздердің тізімі

1. Andrew H. Web Application Security, Sebastopol, California, USA, O'Reilly Media 2020. P. 330
2. Банк данных угроз безопасности информации. Сілтеме мекенжайы: https://data-sec.ru/personal-data/threats-data-bank/
3. Что такое CVE и какие угрозы там хранятся? Сілтеме мекенжайы: https://habr.com/ru/company/pvs-studio/blog/678410/
4. Faircloth J. Penetration Tester's Open Source Toolkit. Oxford, United Kingdom Syngress,
5. Maltego. Сілтеме мекенжайы: https://www.maltego.com/
6. Коротко об SSH. Сілтеме мекенжайы: https://habr.com/ru/sandbox/166705/
7. Pollard B. HTTP/2 in action. Shelter Island, New York, USA, Mannig,2021. P. 424
8. Что такое FTP-сервер и для чего он нужен? Сілтеме мекенжайы: https://galtsystems.com/blog/start/chto_takoe_ftp_server_i_dlya_chego_on_nuzhen/
9. CVE-2022-0739. Сілтеме мекенжайы: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0739
10. Sqlmap . Сілтеме мекенжайы: https://sqlmap.org/
11. CVE-2021-29447. Сілтеме мекенжайы: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29447

ӘОЖ: 004.056

SIEM ЖҮЙЕЛЕРІН ТАЛДАУ ЖӘНЕ ОЛАРДЫ ҚАУІПСІЗДІК САЛАСЫНДА ҚОЛДАНУ. ЖЕДЕЛ АҚПАРАТ ЖӘНЕ ҚАУІПСІЗДІК ОРТАЛЫҚТАРЫ

Манатбек Әбілқайыр Қабибекұлы
abylkaiyr_01_98@mail.ru
Л.Н.Гумилев атындағы Еуразия Ұлттық Университетініңмагистранты, Нұр-Сұлтан, Қазақстан
Ғылыми жетекші - Ахметова Жанар Жумановна

Аннотация: Бизнес мақсаттарына қол жеткізу, бәсекеге қабілеттілікті және заңды қызметті сақтау үшін әртүрлі көлемдегі және қызмет аясындағы барлық типтегі заманауи ұйымдар (мысалы, коммерциялық кәсіпорындар, мемлекеттік мекемелер, коммерциялық емесұйымдар) көптеген ішкі

және сыртқы талаптарға сай болуы керек. Бұл ұйымдар пайдаланушылардың әртүрлі топтары үшін құнды активтерді, бизнестің үздіксіз жұмысын, сенімді деректерді және сараланған қызмет көрсету сапасын (QoS) қамтамасыз етуі керек. Олар өз клиенттері мен қызметкерлерін ұйымның ішінде ғана емес, сыртында да қорғауы керек, осыған байланысты екі жаңа термин енгізілді – телекөрсетілім немесе қашықтан жұмыс. Gartner мәліметтері бойынша, 2025 жылға қарай жаһандық бизнестің 40%-ын киберқылмыскерлердің немесе киберактивистердің тәуелсіз тобы тікелей бұзады. Желіні бұзужағдайларының 60%-ын хакерлер бірнеше минут ішінде бұзады, деп хабарлайды Verizon компаниясының 2022 жылғы деректердің бұзылуын тергеу туралы есебінде. Ұйымдардың Интранет қауіпсіздігін басқарудың интеграцияланған жүйесі бұрын-соңды болмағандай қажет.Осы жүйеде жиналған және талданған деректер оның көзін табу, оның түрін қарастыру, оның салдарын өлшеу, векторын визуализациялау, барлық мақсатты жүйелерді байланыстыру, қарсы шараларға басымдық беру және әсердің маңыздылығын ескере отырып, жұмсарту шешімдерінұсыну үшін кез келген ақпараттық қауіпсіздік оқиғасы (АҚ) тұрғысынан онлайн бағалануы керек. Бұл мақалада қауіпсіздік және оқиғаларды басқару жүйелерінің (SIEM) тұжырымдамасы мен эволюциясы және оларды Интранет АҚ басқару үшін қауіпсіздік операциялары орталықтары мен қауіпсіздікті талдау орталықтарында пайдалану туралы қысқаша талдау берілген.

Кілт сөздер: қауіпсіздік туралы ақпарат және оқиғаларды басқару жүйесі, SIEM, қауіпсіздік операциялары орталығы, қауіпсіздік барлау орталығы.

1. Кіріспе

Ақпараттық қауіпсіздік оқиғасы іскери операцияларға қауіп төндіретін бір немесе бірнеше қажетсіз немесе күтпеген оқиғалар тізбегін білдіреді [1]. Өз кезегінде, IS оқиғасы - бұл жүйенің, қызметтің немесе желінің күйінің анықталған (бақыланатын) пайда болуы. Жүйеге, қызметке немесе желіге кез-келген шабуыл АҚ-мен байланысты оқиға немесе оқиға ретінде жіктелуі мүмкін. Қазіргі уақытта қандай АҚ қауіптері бар екенін, олардың АҚ оқиғасына қалай ұласып, содан кейін ұйымға қалай әсер ететінін білу өте маңызды, әсіресе егер олар жеке меншік пен құпия деректердің ашылуына немесе қызмет көрсетудің үзілуіне, оның беделіне немесе қаржылық әл-ауқатына нұқсан келтіруі мүмкін болса және т. б. 1990 жылдардың аяғында ақпараттарды қорғаудың тиісті құралдары (IPTS) және АҚ инциденттерін жақсы басқарудың негізі болып табылатын білікті персоналы бар қауіпсіздікті басқарудың мамандандырылған орталығы (SOC) пайда болды. Осыдан кейін 2010 жылы желілік деңгейдегі АҚ оқиғаларын және одан да маңызды жоғары деңгейлі АҚ оқиғаларын уақытша қарау үшін бір жерде толық көріну мен бақылауды, сондай-ақ контекстке тәуелді қауіпсіздік аналитикасын қамтамасыз ететін интеграцияланған АҚ архитектурасы бар қауіпсіздікті талдауорталығы (SIC) пайда болды. Көп жағдайда SOC және SIC қауіпсіздік және оқиғаларды басқару туралы ақпарат жүйелеріне (SIEM) олардың ажырамас бөлігі ретінде негізделген.

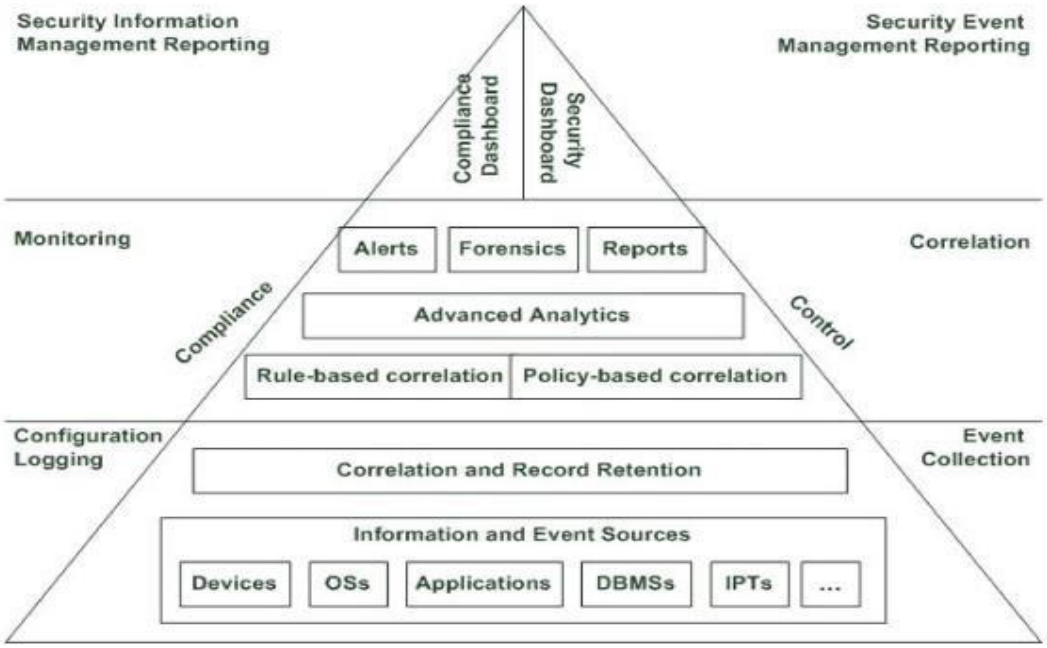
2. SIEM тұжырымдамасы

IPTS бір күн ішінде ірі ұйымның ішкі желілерінде әртүрлі шығу тегі мен салдары бар миллиондаған АҚ оқиғаларын тіркей алады. АҚ оқиғалары тұрғысынан шынымен маңызды деректерді анықтау және АҚ оқиғалары туралы ақпарат алу үшін қажет жұмыс көлемі өте үлкен болуы мүмкін. Өкінішке орай, көбінесе қолмен және көп уақытты қажет ететін бұл әрекет ең тәжірибелі мамандар үшін де қиындық тудыруы мүмкін.

SEM жүйелері оқиғаларды нақты уақыт режимінде жинайды, оларды нақты уақыт режимінде талдайды, хабарламалар жібереді және қорғаныс шараларын тезірек қабылдау үшін оператор консоліне ақпарат береді. Осылайша, SEM жеделдікке бағытталған, ал SIM SIEM жүйелерін талдауды және оларды қауіпсіздік операцияларында пайдалануды тарихи жазбаларды жүргізуге көбірек бағыттайды. Біріктірілген SIEM жүйесі талдау үшін IS-ке қатысты журналдар мен басқа ақпаратты жинайды [2].

SIEM жүйесінің типтік архитектурасы суретте көрсетілген [2]. Суреттің төменгі жағында оқиғаларды жинау мен жазбаларды сақтаудың негізгі мүмкіндіктері көрсетілген. Бұл ортадағы сақталған деректер бақылау және корреляция тапсырмалары үшін пайдаланылады. Жоғарыда талданған деректер қауіпсіздік туралы ақпарат түрінде немесе оқиғаларға негізделген есептерде

ұсынылуы мүмкін екендігі көрсетілген.



Сурет. 1. SIEM жүйесінің типтік архитектурасы.

3. SOC және SIEM 1.0

Басқа IPTS-пен біріктірілген SIEM жүйелері кез-келген ұйым үшін АҚ оқиғаларына бір терезе бола алады. Оқиғалар мен пайдаланушылардың белсенділігін үнемі бақылау үшін қолданылатын SIEM жүйелері АҚ инциденттерін анықтай алады және оларды АҚ тәуекелдерін басқару және осы автоматтандыруды айтарлықтай жақсарту үшін нақты уақыт режимінде машиналық деректердің үлкен көлемін біріктіру арқылы өңдей алады. SIEM жүйелері сонымен қатар жасырын болуы мүмкін интранет ресурстарына төнетін қауіптерді елестете алады. Сондықтан олар SOC ядросы ретінде қарастырылады[3].

SIEM жүйелері интранет АҚ басқаруда келесі мақсаттарға қол жеткізуге көмектеседі [6]:

- Қолданылатын салалық және халықаралық стандарттар мен ережелерге сәйкес интранеттегі және есептіліктегі АҚ талдау қызметін компьютерлендіру;
- Ұйымның ішкі желісіндегі IS деңгейінің нақты жағдайы және белгілі бір активтер туралы ақпарат алу үшін;
- АҚ туындайтын оқиғалар мен инциденттерге ден қоюды жеделдету және қайта анықталған өңдеу және корреляция ережелеріне сәйкес АҚ оқиғаларына автоматты түрде денқою арқылы интранет АҚ-ны тәулік бойы қамтамасыз ету үшін;
- Ұйымда АҚ тәуекелдерін ақылға қонымды бағалауды жүргізу және осы бағалау негізінде АҚ тәуекелдерін уақытылы жою немесе азайту;
- АЖ саласында тиімді шешім қабылдауды рәсімдеу және енгізу;
- АҚ қызметкерлерін оқыту шығындарын азайтылады, өйткені интранеттерде қолданылатын барлық гетерогенді IPT орнына тек осындай жүйенің интерфейсін зерттеу қажет.

1990 жылдардың аяғында SOC-тың ажырамас бөлігі ретінде кеңінен қолданылған бірінші буын SIEM жүйелері (SIEM 1.0) журналға бағытталған және берілген ережелер мен ақпаратты корреляциялау әдістері арқылы IS оқиғаларын анықтады. Мысалы, журналдар әдеттен тыс ұзын сұрау жолдары, рұқсат етілмеген туннельдеу немесе шифрлау туралы ескертуі мүмкін. Бірақ олар контексте белгілі бір клиентті немесе зиянды әрекеттерді анықтауға, TOR сияқты рұқсат етілмеген құралдарды пайдалануға, әдеттен тыс порттар арқылы SSL-ді пайдалануға, стандартты емес желілік трафикке, протоколдың ауытқуларына, рұқсатсыз қосылымдарға және т.б. анықтауда дәрменсіз болды. Verizon компаниясының 2015 жылғы деректердің бұзылуын тергеу есебіне сәйкес, сәтті шабуылдардың 99% - ы журналдардың назарынан тыс қалды [7]. SIEM 1.0-дің тағы бір маңызды кемшілігі - келесі шектеулері бар реляциялық мәліметтер базасын пайдалану: шамалы

семантикалық байлық және өте қарапайым құрылымдар, Рекурсия мен мұрагерлікті қолдаудың болмауы, триггерлердің болмауы және т.б. SIEM 1.0-дің барлық кемшіліктері келесі буын SIEM жүйелерін дамыту қажеттілігіне әкелді.

4. SIC және SIEM 2.0

Жиі және күрделі шабуылдардың жаңа шындығы және "қызмет ретінде бұзу" интранеттерді кәсіби бұзуды қол жетімді және қауіптің жоғарғы деңгейін көрсетеді. Көптеген ұйымдар бұл мәселеге қатысты деректерді талдау жеткіліксіз екенін түсіне бастайды; олар осыған байланысты шаралар қабылдауы керектігін түсінді. Сол себепті әзірленген және орталықтандырылған АҚ басқару жүйелерін ұйымдастыруға ден қойды.

Мұндай тәсілді жүзеге асыру және барлық күнделікті операцияларды барынша автоматтандыру және сараптамалық шешімдер қабылдауды қажет етпейтін АҚ инциденттеріне жауап беру үшін кез-келген заманауи ұйым осы міндеттерді шешетін және дәстүрлі SOC-қа қарағанда жетілдірілген АҚ басқару орталығын құруы керек. Интеграцияланған шабуылдан қорғау архитектурасы бар SIC деп аталатын желі деңгейіндегі оқиғаларды және одан да маңызды жоғары деңгейлі АҚ оқиғаларын уақытша өңдеу үшін толық көріну мен бақылауды, сондай-ақ бір жерде контекстке тәуелді қауіпсіздік аналитикасынқамтамасыз етеді.

2000 жылдардың соңында іске қосылған екінші буын SIEM жүйелері (SIEM 2.0) контекстік талдауды орындайды және келесі негізгі функцияларды орындайды:

1. Нақты уақыт режимінде анықтау және интранеттің барлық таратылған гетерогенді көздерінен АҚ оқиғалары туралы ақпаратты орталықтандырылған жинау: IPTS (бағдарламалық жасақтама және аппараттық құрал), желілік құрылғылар, қосымшалар, мәліметтер базасы, конфигурация файлдары және т. б.;
2. Белгілі бір контексте пайдаланушы мен қолданба әрекетін бақылау;
3. иналған ақпаратты (оның ішінде сүзу, жинақтау, қалыпқа келтіру, корреляция және т. б.) Пайдаланушының және қосымшаның алдыңғы және ағымдағы белсенділігін және жинақталған статистиканы ескере отырып, белгілі бір контексте өңдеу;
4. Әрбір АҚ инцидентінің бүкіл өмірлік циклін қадағалау жіктелген АҚ оқиғаларына жауап ретінде белгілі бір әрекеттерді талдау және автоматты түрде орындау;
5. Big Data ақпараттық технологияларын жадта және дерекқорда аналитикамен, жаппай параллельді бағдарламалаумен және т.б. (реляциялық мәліметтер базасының орнына) масштабталатын IS аналитикасы үшін пайдалану. Мұның бәрі SIC-те болғандықтан, ұйымдар келесі негізгі артықшылықтарға ие болады:

- АҚ тәуекелдерін басқаруды АҚ-ның алдын ала анықталған маңызды көрсеткіштері және 24/7 қауіпсіздікті қамту негізінде бизнестің қажеттіліктерімен үйлестіру, жергілікті мониторингті бақылауды, үздіксіз тіркелетін оқиғалар, сыртқы және ішкі қауіптерді талдауды, бірыңғай көрініс өтпелі көрінуді және пайдаланушылар арасындағы жасырын өзара байланыстар мен күдікті бірлестіктерді анықтау үшін объектілермен байланыстарды талдауды, есептік жазбаларды немесе басқа ұйымдарды біріктіреді. олардың өмірлік циклінің алғашқы кезеңдері бір жерде, толық уақытты кадрлармен қамтамасыз етуді қажет етпейді;
- Неғұрлым жақсы тәсіл өз ресурстарын желілік қауіпсіздіктің нақты қауіптеріне шоғырландырады, әскери істен алынған "тереңдетілген қорғаныс" стратегиялары болып табылатын және осы деңгейлерді стратегиялық түрде ұйымдастыратын АҚ-ның артық көптеген деңгейлеріне басымдық береді.

5. Қорытынды

Қазіргі уақытта тіпті SIC идеясы өте гетерогенді өзара байланысты әлемде төнетін қауіптердің көбеюіне ілесе алмайды. Бұрын-соңды болмағандай, ұйымдардың ИТ активтерінің қауіпсіздігін қамтамасыз ету үшін тиімді IS басқару құрылымын құрудың келесі эволюциялық қадамы күтілуде. Біздің ойымызша, бұл прогрессивті құрылым SIC – тің барлық артықшылықтарын NOC желілік операциялық орталықтарында жүзеге асырылған желілік операцияларды басқарудың көп жылдық тәжірибесімен біріктіруі керек.

Пайдаланылған әдебиеттер тізімі

1. ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary (2016)
2. IBM Corporation: IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager. 2nd edn. (2010). http://www.redbooks.ibm.com/abstracts/sg247530.html?Open.
3. Techtarget: Security information and event management (SIEM) (2014). http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM.
4. Scarfone, K.: Introduction to SIEM services and products (2015). http://searchsecurity.techtarget.com/feature/Introduction-to-SIEM-services-and-products.
5. Miller, D., Harris, S., Harper, A., VanDyke, S.: Security Information and Event Management (SIEM) Implementation. McGraw-Hill, New York (2010). 464 p.
6. Miloslavskaya, N.G., Senatorov, M.Y., Tolstoy, A.I.: Information Security Incident and Business Continuity Management. Information Security Management Issues Series, 2nd edn., vol.3,170 p. Goriachaja linia-Telecom, Moscow (2014).
7. Verizon: Data Breach Investigations Report (2015). http://www.verizonenterprise.com/DBIR/2015/.

УДК: 004

ИССЛЕДОВАНИЕ МЕТОДОВ КЭШИРОВАНИЯ ПРИ УПРАВЛЕНИИ ДАННЫМИ

Марат Марта Мараткызы
магистрант 2 курса специальности «Информационные системы» maratkyzy.m@gmail.com,
научный руководитель, доктор философии (PhD), и.о.доцент кафедры Информационные системы
Касекеева А.Б.
ЕНУ им Л.Н. Гумилева, г. Астана

Аннотация

В этой работе рассмотрены известные алгоритмы кэширования. Была построена аналитическая модель системы кэширования. Также был предложен и реализован алгоритм, особенностью которого является учет нагрузки на сеть необходимой для повторной передачи данных при их вытеснении из кэша. Были проведены сравнения эффективности алгоритмов на различных тестовых наборах.

Введение

Первой технологией, которая использовалась с целью снижения времени ожидания ответов от сервера на запросы пользователей и снижения трафика, было кэширование. Постоянное развитие сетевых технологий и глобальной сети Интернет обуславливают рост числа исследований во всем мире направленных на повышение производительности систем, основанных на данных технологиях. Одним из основных направлений исследований является использование кэширования как главного инструмента для снижения нагрузки на систему в целом, увеличения ее производительности. Обычно кэширование определяется как хранение ответов на запросы с целью их последующего повторного использования[1]. Кэширование преследует следующие цели:

- сократить время ожидания ответа пользователем;
- уменьшить нагрузку на сервер;
- уменьшить нагрузку на сеть.

Аналитическая модель кэширования

Аналитическая модель системы кэширования позволяет понять структуру системы и связи между ее отдельными элементами. С ее помощью могут быть оптимально определены параметры настройки системы для достижения максимальной эффективности.

Было замечено, что распределение относительной частоты запросов соответствует закону Зипфа [2], который гласит, что если все запросы упорядочить по убыванию частоты их