ӘОК:273.08048

DLP ЖҮЙЕЛЕРІНІҢ ҚҰРЫЛЫМЫ

Зәйнікен Аяулым
azainiken@gmail.com
Ақпараттық технологиялар факультетінің 1 курс магистранты
«Л. Н. Гумилев атындағы Еуразия ұлттық университеті» ШЖҚ РМК,
Нұр-Сұлтан, Қазақстан
Ғылыми жетекшісі – Қонырханова А.А.

Аңдатпа: Құпия деректер көптеген компаниялар үшін өте маңызды актив көзі болып табылады, сондықтан бұл деректерді қорғауға компанияның жоғарғы басшылығы, әкімшілер және IT-менеджерлер көп көңіл бөледі. Деректердің ағуы компанияларға теріс әсер етеді. Брандмауэр сияқты қауіпсіздіктің дәстүрлі тәсілдері деректерді ағып кетуден қорғай алмайды. Деректердің ағып кетуін / жоғалуын болдырмау жүйелері (DLP) – құпия деректерді сенімсіз қолдарға түсуден қорғайтын шешімдер болып табылады. Бұл мақала DLP жүйелеріне шолу жасауға және олардың құрылымын зерттеуге тырысады.

Түйінді сөздер: DLP жүйелері, ақпараттық қауіпсіздік, Data Leak Prevention.

Кіріспе

Заманауи әлемде, ақпарат аса құнды дерек көзі болып табылады. Жаңа ақпараттық технологиялардың пайда болуы және ақпаратты сақтау мен өңдеудің қуатты компьютерлік жүйелерінің дамуы, ақпаратты қорғау деңгейіне қойылатын талаптарды арттырды және қазіргі заманғы деректерді сақтау архитектурасына бейімделген ақпаратты қорғаудың тиімді механизмдерін әзірлеу қажеттілігін туғызды.

Әр түрлі типтегі компаниялар өз қызметін сақтау үшін, құпия ақпаратқа рұқсатсыз қол жеткізуден аулақ болу үшін көптеген әдіс-тәсілдерді қолдануға тырысады. Ақпараттың таралуынан қорғау құралдарына әр түрлі антивирустық бағдарламалар, брандмауэрлер және тағы басқа бағдарлама құралдары жатады.

Әр түрлі типтегі компаниялар өз қызметін сақтау үшін, құпия ақпаратқа рұқсатсыз қол жеткізуден аулақ болу үшін антивирустық бағдарламаларды, брандмауэрлерді, SIEM, IPS/IDS, DLP жүйелерін қолданады. Бұл мақалада ақпараттық қауіпсіздікті қамтамасыз ететін DLP жүйелері қарастырылады.

DLP жүйелерінің құрылымы

DLP (Data Leak Prevention) - бұл деректердің ағып кетуін алдын алуға және жол бермеуге арналған бағдарламалық және аппаратты-бағдарламалық жасақтама құралдары.

Жүйені пайдаланудың негізгі мақсаты – құпия деректердің, ақпарттық жүйеден сыртқа ағып кетуінен қорғау болып табылады.

DLP-кешендері ұйымның айналасында барлық шығыс және кіріс деректерін талдауға мүмкіндік береді. Ол тек қана интернет-трафикті ғана емес, сонымен қатар қауіпсіздік периметрінен тыс шығарылатын ақпарат ағындарының басқа түрлерін де тексереді.

Ақпараттың ағып кетуінен қорғайтын DLP жүйелерінің негізгі функцияларына:

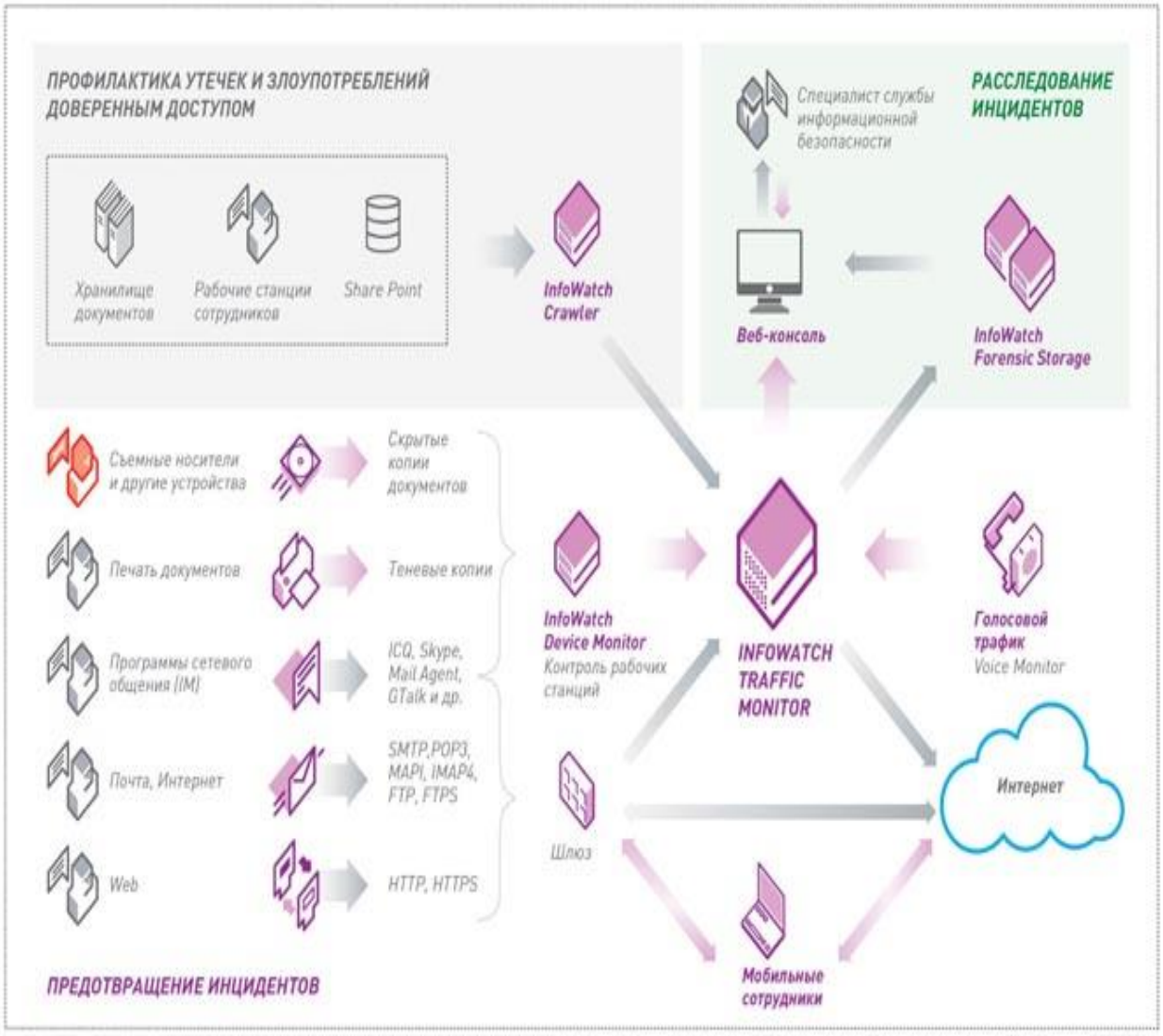
– Ақпаратты интернет арқылы, оның ішінде E-Mail, Telegram, Skype және т.б. қосымшалар, сонымен қатар әр түрлі желілік хаттамаларды пайдалану кезінде беруді бақылау;

– DVD, флэш-дискілер, телефондар, смартфондар және т.б. құралдарда ақпараттың сақталуын бақылау;

– басып шығаруға жіберілетін мәліметтерді бақылау;

– ақпараттық қауіпсіздік әкімшілеріне рұқсат етілмеген инциденттердің орындаоғандығы туралы хабарлау;

– файл серверіндегі және қызметкерлердің жұмыс орнындағы ұұпия ақпараттарды - кілт сөздер, құжаттар тегі, файл атрибуттары және сандық басылымдар арқылы іздеу жатады (Сурет 1).



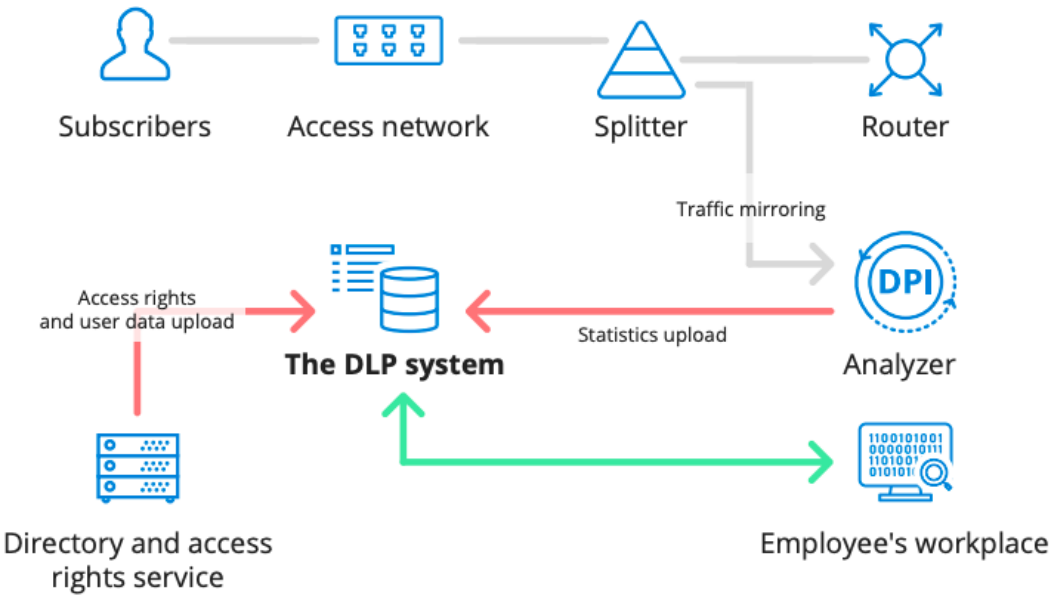
Сурет 1. DLP жүйелерінің негізгі функциялары

DLP жүйесі үш бөліктен тұрады. Бұл компания қызметкерлерінің агенті, сервері және желілік арналар арқылы берілетін құпия ақпаратты бақылау және бұғаттау компоненттері (Сурет 2).

Агент - агент пайдаланушылардың компьютерлеріне орнатылады және пайдаланушының әр әрекетін серверге жібереді. Серверге жіберілетін деректер жүйеде анықталған қауіпсіздік саясаты негізінде жүзеге асырылады.

Сервер - агенттен келген барлық деректер серверде сақталады және өңделеді. Өңделген деректер деректер базасынан қауіпсіздік маманына ыңғайлы көріністегі есептеме түрінде жіберіледі.

Желілік арналар арқылы берілетін құпия ақпаратты бақылау және бұғаттау - бұл компонент шлюз арқылы ақпараттың қозғалысын бақылауға жауап береді. Кез келген TCP/IP немесе UDP арнасы бойынша ақпарат беруді қадағалауды жүзеге асырады. Жүйе IM және пирингтік жүйелер арқылы ақпарат алмасуды бақылайды, сондай-ақ пайдаланушыларды корпоративтік саясаттың бұзылғаны туралы хабардар ету мүмкіндігімен HTTP, FTP және SMTP-арналары арқылы ақпарат жіберуді бұғаттауға мүмкіндік береді.



Сурет 2. Корпоративтік желідегі DLP жүйелері

DLP жүйесі келесі модульдерді қамтиды:

Басқару тақтасы - негізгі панель. Негізгі деректер мен статистика графиктер түрінде ұсынылады. Бұл модуль деректерді ыңғайлы қарауға мүмкіндік береді. Белгілі бір уақыт аралығында қызметкерлер жинаған және талдаған мәліметтер ұйымның қауіпсіздік қызметкерлеріне ыңғайлы түрде ұсынылады. Сервер статистикасын да көруге болады.

Қызметкерлер ең маңызды модульдердің бірі болып табылады. Бұл модуль қызметкерлердің тізімін және олар туралы ақпаратты ұсынады. Оларға қызметкерлердің аты-жөндері, компьютер атаулары, mac мекенжайлары, қызметкерлердің мәртебесі, бөлімдер, лауазымдар және т.б. кіруі мүмкін. Сондай-ақ, сіз әр қызметкер үшін апта сайынғы, айлық немесе жылдық статистикалық мәліметтерді көре аласыз.

Компьютерлер - бұл жүйені құру үшін қажетті негізгі құралдар. Себебі ол жүйенің негізгі бөлігі болып табылатын агент пен қызметкерлердің компьютерлерін орнатады. Бұл модуль әр түрлі ішкі модульдерге бөлінеді [4]:

Keylogger - бұл модуль қызметкерлер пернетақтадан енгізген ақпаратты көрсетеді.

Алмасу буфері - бұл модуль көшірілген деректер туралы ақпаратты сақтайды.

USB - бұл қызметкердің флэш-дискісіне көшірілген файлдарды және сол флэш-диск туралы ақпаратты сақтайтын модуль.

Баспа құжаттары - бұл модуль принтермен басылған ақпаратты көрсетеді.

Скриншоттар - бұл модуль қызметкердің компьютерінің немесе планшеттерінің скриншоттарын тұрақты уақыт аралығында сақтайды.

Интернетті пайдалану - бұл модуль қызметкер кірген сайттар туралы ақпаратты, шолғышта іздеген ақпаратты көрсетеді, пошта арқылы жіберілетін ақпарат.

Әлеуметтік желілер - бұл модуль қызметкердің әлеуметтік желілердегі хат-хабарларын, жіберілген және алынған файлдарды көрсетеді.

Саясат - әр ұйым өзінің жүйелік саясатын өз талаптары негізінде орнатады және осы саясатты басқаруға мүмкіндік беретін параметрлер бар. Бұл модульде қызметкерлерді, процестерді, пайдаланушыларды, веб-сайттарды топтастыруға болады.

Инциденттер – бұл модуль ұйым қызметкерлерінің қауіпсіздік саясаты модулінде жазылған заңдарға қайшы келетін әрекеттерін сипаттайды.

Файл анализаторы – бұл модуль қызметкерлердің компьютерлерінде сақталған файлдарды сақтайды және оларды белгіленген тәртіппен талдайды.

Есеп беру - Негізгі модульдердің бірі болып табылады, жүйе қызметкерлер жазған оқиғалар негізінде есептерді автоматты түрде дайындайды. Есеп қарапайым мәтін, кесте немесе диаграмма түрінде ұсынылуы мүмкін.

Параметрлер - Бұл модульде жүйелік параметрлердің әртүрлі түрлері сақталады, мысалы: дерекқорды басқару-одан көшіру, жүйелік дерекқорды өзгерту. Агент жаңартулары, хабарландырулар, желі параметрлері.

Кілт сөздер – кілт сөздерді әр ұйым қауіпсіздік саясатының негізінде анықтайды.

Журналдар – бұл модуль жүйенің өзіне байланысты қызметкерлердің кіру уақытын және қызметкер мен жүйенің әртүрлі әрекеттерін сақтай алады.

Қорытынды

Сандық және әлеуметтік инженерияның дамуы құпия ақпараттың қауіпсіздігіне қойылатын талаптарды арттырды. Бүгінгі таңда ақпараттық қауіпсіздікті қамтамасыз етудін сенімді жүйелерін таңдау өте маңызды мәселелердің бірі болып табылады. Қорғалатын ақпарат таралып кеткен жағдайда, кәсіпорын қаржы саласында шығынға ұшырайды және көпжылдық беделге қауіп төнеді. Кәсіпорын жүйесінің ағып кетуінен қауіпсіздікті қамтамасыз етуге мүмкіндік беретін шешімнің бірі DLP жүйелерін пайдалану болып табылады.

Қолданылған әдебиеттер тізімі

1. Polozova E., Anashkina N. Analysis of information security threats for developing DLP-systems // production engineering archives 17 (2017) 25-28.
2. V. Clincy and H. Shahriar, "Web Application Firewall: Network Security Models and Configuration," 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), 2018, pp. 835-836, doi: 10.1109/COMPSAC.2018.00144.
3. Yulchiyev Ibrokhimjon Usmonali o’g’li. (2021). DLP system overview. Texas Journal of Multidisciplinary Studies, 3, 166–167.
4. Miloslavskaya N., Morozov V., Tolstay A., Khassan D. DLP as an integral part of network security intelligence center // 2017 IEEE 5th international conference on future internet of things and cloud (ficloud).