ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

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 имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

пайдалану мақаласында, Майоровтың Заманауи VPN желілері мақаласында белгілі бір саладағы емес, жалпы VPN желісіне талдау жасаған.

Қазіргі уақытта дүние жүзіндегі көптеген телекоммуникациялық ұйымдар жоғарыда аталған қиындықтар мен талаптарды шешу үшін қауіпсіз және заманауи VPN шешімдерін қолданады. Дәлел ретінде Халықаралық электрбайланыс одағы (ITU) және Телекоммуникация индустриясы қауымдастығы (TIA) сияқты жетекші салалық ұйымдар телекоммуникация желілеріндегі деректердің қауіпсіздігі мен құпиялылығын арттыру үшін VPN желілерін пайдалануды жақтайды. Cisco, Palo Alto Networks және Fortinet қоса алғанда, желілік және киберқауіпсіздік кеңістігінде қалыптасқан жеткізушілер телекоммуникация ұйымдары үшін арнайы әзірленген, жоғары өнімді шифрлау, масштабтау және сияқты мүмкіндіктері бар кеңейтілген VPN шешімдерін ұсынады. Қолданыстағы желілік инфрақұрылыммен интеграция. Еуропадағы GDPR немесе Америка Құрама Штаттарындағы Медициналық сақтандыруды тасымалдау және есеп беру актісі (HIPAA) сияқты деректерді қорғау ережелеріне сәйкестік телекоммуникация ұйымдарында VPN сияқты қауіпсіз байланыс арналарын енгізуді қажет етеді. Осы ережелерді сақтау VPN пайдаланудың күшті көрсеткіші болып табылады[4].

Қорытындылай келе, телекоммуникация ұйымдары үшін қауіпсіз және заманауи VPN маңыздылығын асыра айту мүмкін емес. Ол құпия деректерді қорғауда, нормативтік талаптардың сақталуын қамтамасыз етуде, киберқауіптерден қорғауда, қашықтан қол жеткізуге мүмкіндік беруде және желі өнімділігін арттыруда маңызды рөл атқарады. Телекоммуникация индустриясында VPN шешімдерін кеңінен қолдану олардың қауіпсіздік пен операциялық маңызды мәселелерді шешудегі дәлелденген тиімділігін көрсетеді.

Қолданылған әдебиеттер тізімі

1. Исмаэль Буарфа, Жетілдірілген цифрлық қорғауға арналған корпоративтік VPN архитектурасы, 2022ж., қол жеткізу режимі: https://medium.com/@ismaelbouarfa/corporate-vpn-architectures-for-enhanced-digital protection-517b68a2daa8 (қаралған күні 17.03.2024).
2. Винсент Х. Хиндман, Жетілдірілген цифрлық қорғауға арналған корпоративтік VPN архитектурасы, 2022ж., қол жеткізу режимі: https://www.pqmconsultants.com/vpn/ (қаралған күні 18.03.2024).
3. Ұйымға арналған виртуалды жеке желіні жобалау және енгізу, 2019 ж., қол жеткізу режимі: https://www.lawyersnjurists.com/article/design-implementation-virtual-private-network-organization/ (қаралған күні 18.03.2024).
4. А.Ю. Николахин, АҚПАРАТ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ҮШІН VPN ТЕХНОЛОГИЯСЫН ПАЙДАЛАНУ, қол жеткізу режимі: https://nirit.org/wp-content/uploads/2018/12/60-68.pdf (қаралған күні 19.03.2024)

ӘОЖ 004.056

АВТОМАТТАНДЫРЫЛҒАН ЖҮЙЕЛЕРДЕ ДЕРБЕС ДЕРЕКТЕРДІ ҚОРҒАУДА ЕКІ ФАКТОРЛЫ АУТЕНТИФИКАЦИЯ ҚОЛДАНЫСЫ

Жансейітова Мөлдір Әбдірзаққызы
zhanseiitovamoldir@gmail.com
Л.Н.Гумилев атындағы Еуразия ұлттық университетінің Ақпараттық қауіпсіздік кафедрасының магистранты, Астана, Қазақстан
Ғылыми жетекші – Сантеева С.Ә.

Аңдатпа: Бұл жұмыс екі факторлы аутентификация әдістерін сипаттайды және оны автоматтандырылған басқару жүйесіндегі қолдану тиімділіктерін, артықшылықтарын қарастырады.

Кілттік сөздер: ақпараттық қауіпсіздік, 2FA (екі факторлы аутентификация),фишинг,аутенфикация.

Қазіргі таңда аутентификациялық ақпараттық жүйелерді қорғау және оларды сақтандыру жұмыстары өзекті болып табылады, өйткені олар әртүрлі мекемелердің жүйелерінде тұтынушылардың деректерін жазу, өңдеу және сақтау үшін қолданылады. Сол себептен де, ақпараттық жүйелерді қорғауды арттыру мақсатында аутентификацияның қосымша қауіпсіздік шаралары арқылы пайдаланушының деректерді сақтауы қазір де өзекті мәселе.

Қоғамды ақпарат алмасудың, берудің және сақтаудың негізгі құралы болып табылатын ақпараттық ресурстарсыз елестету мүмкін емес. Жаһандық ақпараттандыру дәуірінде кез келген бағыттағы әрбір дерлік жеке меншік мекемелер электрондық құжат айналымының ақпараттық жүйелерін пайдаланады.

Ақпарат – деректерді өңдеу және сақтау үшін қолданылатын негізгі объект. Кез-келген ақпараттың белгілі бір құндылығы бар, сондықтан шабуылдаушылардың мәліметтерді алуы белгілі бір кірісті қамтамасыз етеді [1]. Шабуыл жасаушының негізгі мақсаты - субъектінің әрекеттері туралы құпия деректерді алу. Әдетте, шабуылдаушыларды экономикалық ақпаратты қамтитын ақпарат, қызметкердің, клиенттің, сатып алушының жеке деректері, объектінің мүлкі, бәсекелестердің қызметі туралы зерттеулер, төлем жүйелерінің әдістері мен құралдары қызықтырады.

Қазір заманауи ақпараттық жүйелерді талдау, ақпараттық жүйеде сақталатын және өңделген деректердің қолжетімділігін, тұтастығын және құпиялылығын қорғау үшін қосымша тосқауыл ретінде екі факторлы аутентификацияны пайдалану қажеттілігі өте жоғары. Бұл қолданбалы әдіс – аутентификаторлар және мобильді қосымшаларды пайдалана отырып, логинді тексеру арқылы екі факторлы аутентификацияның ақпараттық жүйені толық бағдарламалық деректерді қамтамасыз енгізу үшін қауіпсіз, әрі практикалық ыңғайлы екені анықталған[2].

Бәсекелестердің немесе шабуылдаушылардың негізгі мақсаты - құпия қызығушылық объектілерінде айналатын деректердің құрылымына өзгерістер енгізу. Мұндай әсер ету деректермен жұмыс істеу кезінде белгілі бір салада жалған ақпаратқа әкелуі мүмкін. Ең қауіптісі – бағдарламалық қосымшалардағы жиналған деректер массивін жою болып саналады. Талқыланған оқиғаларға байланысты ақпараттық қауіпсіздіктің тиімді тұжырымдамаларын қалыптастыру үлкен маңызға ие[2].

Көптеген салаларда веб-әзірлеудің логикалық қателіктері қауіпсіздік мәселесіне әкелуі мүмкін немесе күтпеген торап әрекеттеріне әкеледі. Дегенмен, аутентификациялық қауіпсіздік жүйесі маңыздырақ болғандықтан, аутентификацияның мықтылығы веб-сайттың қауіпсіздік мәселелерін айтарлықтай төмендетуге ықтималдылығы зор. Ал аутентификациядағы осалдықтардың салдары өте ауыр болуы мүмкін. Шабуылдаушы аутентификацияны айналып өткенде немесе басқа пайдаланушының деректерін бұзған кезде, олар бұзылған тіркелгідегі барлық деректер мен функцияларға қол жеткізе алады. Жүйе әкімшісі сияқты жоғарғы тіркелгіні бұзып үлгерсе, олар бүкіл деректерді толық бақылауға және ішкі инфрақұрылымға кіру мүмкіндігіне ие бола алады.

Төменде жалпы әлсіз аутентификация шабуылдарына әкелетін негізгі қауіп көздері берілген[1].

1) Осал аутентификация логикасы
2) Тіркелгі/парольді қалпына келтіру процесі әлсіз
3) Осал аутентификация кітапханасын пайдалану
4) Қауіпті сеанс өңдеу
5) Жылдамдықты шектегіштер немесе процесті блоктау жоқ
6) Қауіпті аутентификациялық тіркелу.

Логикалық кемшіліктерді пайдалану күрделірек және қолмен енгзу әдісін қажет етеді, бірақ әлсіз құпия сөздерден және белгілі кітапханаға тәуелділік осалдықтарынан туындаған кемшілітерді пайдалану оңай. Бірақ ең ықтималды қауіп пайдаланушыларды тіркелгі

деректерінен бас тартуға мәжбүрлеу. Оларды аутентификация процесін екі жолмен бұзу үшін жиі қолданылатын шабуылдар ретінде жіктеуге болады[3]:

1) Құпия сөзді бұзу: Фишинг – пайдаланушыларды құпия сөздер мен PIN кодтары сияқты тіркелгі деректерінен бас тартуға алдап соғудың танымал әдісі және ең күшті шабуыл векторларының бірі болып табылады. Фишинг көптеген басқа шабуыл векторларына қарағанда жоғары табысқа ие, бұл оның танымалдылығын түсіндіреді.

2) SQL инъекциясы: SQL инъекциясы аутентификацияланбаған деректерді, рұқсат етілмеген деректерді шығара алатын немесе тіпті қолданбаның логикалық әрекетін өзгерте алатын өңделмеген SQL сұрауларын енгізуді қамтиды. Аутентификация контекстінде SQL инъекциясы дерекқорда сақталған тіркелгі деректерін жайып жіберуі немесе аутентификация логикасына әсер етуі мүмкін, бұл шабуылдаушыға аутентификациясыз кіруге мүмкіндік береді.

Бүгінде 5 миллиардтан астам мобильді құрылғылар қолданылуда және телефонды аутентификация құралы ретінде пайдалану қосымша шығындар мен жеткізу кідірістерін азайта отырып, күшейтілген қауіпсіздік қажеттіліктерін жылдам шешуге көмектеседі. Ақпараттың жайылып кету проблемасы бүкіл әлемде өзекті болып табылады және ақпаратты қорғау үшін екі факторлы аутентификацияны қолдану шабуылдаушылар үшін қосымша тосқауыл болады. Екі факторлы аутентификация әдістері аутентификаторлардың күшін күшейтетін механизмдер ретінде қарастырылады. Екі факторлы қорғаныс – бұл басқа адамдардың деректеріне қол жеткізуді қиындататын және классикалық құпия сөзді қорғаудың кемшіліктерін белгілі бір дәрежеде жоятын жеткілікті сенімді кедергі[2]. Сонымен қатар, тағы бір артықшылығы, екі факторлы аутентификация әдістері өте көп:

1) Нақты дербес компьютерді анықтауға арналған бағдарламалық құрал. Компьютерге арнайы бағдарлама орнатылған, ол оған криптографиялық белгіні енгізеді. Осыдан кейін аутентификация үшін компьютерге орнатылған таңбалауыш пен құпия сөз қажет болады.

2) Биометрия. Адамның физикалық ерекшеліктерін тану арқылы (саусақ ізі, көз және т.б.) биометрия сәйкестендіруде қосымша компонент ретінде қолданылады.

3) Электрондық пошта немесе SMS арқылы бір реттік пароль.

4) Бір реттік пароль белгісі. Пайдаланушы үнемі өзгеретін құпия сөздерді жасайтын құрылғымен қамтамасыз етілген. Дәл осы құпия сөздерді пайдаланушы аутентификация процесінде әдеттегі құпия сөздерге қосымша енгізеді.

5) Сыртқы бақылау. Бұл тәсіл банктің алдын ала тіркелген телефон нөміріне қоңырау шалуын қамтиды.

6) Гаджеттердің көмегімен сәйкестендіру. Сәйкестендірудің бұл түрі кез келген пайдаланушы құрылғысына криптографиялық тегті қою арқылы жүзеге асырылады (мысалы, USB дискісі, iPad, жад картасы және т.б.).

7) Скретч қабаты бар карта. Пайдаланушыға тек бір рет пайдалануға болатын PIN коды бар карта беріледі.

Сараптамаға сәйкес, көп мекемелерде электрондық пошта немесе SMS арқылы уақытша құпия сөздерге негізделген екі факторлы аутентификация шешімдері және басқа да белгілер түрлері жиі қолданылады. 1-суретте екі факторлы аутентификация статистикасы келтірілген.

1-сурет – Екі факторлы аутентификация статистикасы

Қазіргі уақытта тәжірибеде көрсеткендей, барлық дерлік мекемелерде маңызды ресурстар мен қызметтерге екі факторлы аутентификация әдістері пайдаланады. Көптеген компаниялар мен веб-сайттар оны қалыпты кіру процесіне қосымша қауіпсіздік шарасы ретінде қарастырады.

Негізгі артықшылықтары[4]:

- Екі факторлы немесе көп факторлы аутентификацияның ең айқын артықшылығы – қауіпсіздік болып табылады. Есептік жазба неғұрлым қауіпсіз болса, соғұрлым оны ұрлау қиынырақ болады. Шабуылшылар үшін екі құпия сөз екі есе көп жұмысты білдіреді.

- Тағы бір маңызды артықшылық - қол жетімділік және бірнеше құпия сөздерді есте сақтау қажеттілігінен туындаған стрессті азайту. Кейбір жағдайларда сарапшылар бұл операциялық шығындардың төмендеуіне және өнімділіктің артуына әкелуі мүмкін дейді.

-Үшінші маңыздылығы – құрамдас компания ішінде белгілі бір стандарттарды сақтау. Стандартты кіру процедурасы бар мекемелердің қауіпсіздік мәселелеріне тап болу ықтималдығы аз.

Бірақ алдымен,екі факторлы аутентификацияны пайдалану үшін пайдаланушы бірінші фактор ретінде құпия сөзді және басқа, бөлек элемент, көбінесе қауіпсіздік белгісі немесе саусақ ізі немесе бет сканері сияқты биометриялық факторды енгізуі керек. Қолданбаға немесе провайдерге байланысты бірнеше екі факторлы аутентификация опциялары қолжетімді болуы мүмкін. Дегенмен, жалпы көп сатылы екі факторлы аутентификация процедуралары бірдей:

1) Қолданба немесе веб-сайт пайдаланушыны жүйеге кіруге шақырады.

2) Пайдаланушы өзіне таныс деректерді, көбінесе оның тіркелген аты мен паролін енгізеді. Содан кейін веб-сайт сервері сәйкестікті тауып, пайдаланушыны таниды.

3) Веб-сайт пайдаланушы үшін құпия сөзді қажет етпейтін процедуралар үшін арнайы қауіпсіздік кілтін жасайды. Кілт аутентификация механизмімен өңделеді және сайт серверімен тексеріледі.

4) Осыдан кейін веб-сайт пайдаланушыдан екінші кіру процесін бастауды сұрайды. Пайдаланушы биометрикалық, қауіпсіздік белгісі, жеке куәлік, смартфон немесе басқа мобильді құрылғы сияқты тек өзіне ғана тиесілі нәрсеге ие екенін көрсетуі керек, бірақ бұл қадам әртүрлі формада болуы мүмкін. Бұл меншік немесе мұрагерлік фактор.

5) Екі факторды енгізгеннен кейін пайдаланушы аутентификацияланады және қолданбаға немесе веб-сайтқа қол жеткізе алады.

Сонымен біз ең танымал аутентификациялардың бірнешеуін және олардың мүмкіндіктерін қарастырамыз. Барлық қосымшалардың негізгі функциясы бірдей болғанына қарамастан бір алгоритмді пайдаланып бір реттік кодтарды жасау секілді, бірақ кейбір аутентификаторларда қосымша функциялар немесе интерфейс мүмкіндіктері бар.

Қысқаша салыстыра кетсек, 1-кестеде келтірілді[4]:

Аутентификация	Google Authenticator	Duo Mobile	Microsoft Authenticator	FreeOTP	Authy	Yandex.Key
Тәуелсіздік	+	+	+	+	+	+
Қажеттіліктерді синхрондау	+	+	+	+	+	+
Қалпына келтіруді автоматтандыру	-	+	+	+	-	-
Екінші аутентификация әдісі	+	-	-	-	-	+
Қолданбаны қорғау құпия сөзі	-	-	-	+	-	+

Пернетақтадан енгізу	+	+	+	+	+	+
Қолдану мүмкіндігі	-	-	-	-	-	+
Тіркелу қажеттілігі	+	+	+	+	+	+
Құпия трансфер қызметі	+	+	+	+	+	+

Кесте 1– Екі факторлы аутентификацияға арналған қосымшалардың сипаттамалары

Қысқаша айтқанда, шағын бизнеске арналған екі факторлы аутентификация арқылы жеке деректерді қорғау шағын бизнес үшін деректер қауіпсіздігін жақсартуда маңызды қадамдар жасайды. Екі факторлы аутентификацияны (2FA) қосымшаға сәтті әзірлеу және біріктіру оның жеке деректерді қорғаудағы тиімділігін арттырады.

Екі факторлы аутентификация механизмін енгізу арқылы жоба рұқсатсыз кіруден және ықтимал деректердің таралып кетуінен қорғаудың қосымша деңгейін қамтамасыз ететін дәстүрлі құпия сөзге негізделген қауіпсіздік шараларынан асып түседі. Бұл енгізу шағын бизнестің кеңейтілген деректерді қорғауға деген маңызды қажеттілігін шешеді және киберқауіпсіздік қатерлерімен байланысты тәуекелдерді азайтады. Екі факторлы аутентификация және шифрлауды енгізу бизнеске сенім арттыруға және тұтынушылар деректерінің құпиялылығын сақтауға мүмкіндік береді, осылайша берушілермен пайдаланушылардың қарым-қатынастарын нығайтуға көмектеседі.

Қолданылған әдебиеттер тізімі

1. Екі факторлы аутентификацияны орнату, Citrix, 2020: [Онлайн]. Қолжетімді: http://support.citrix.com/proddocs/topic/web-interface-impington/nl/ru/wi-configure-twofactor-authentication-gransden.html?locale=ru. (қаралған күні 17.03.2024).
2. Ding Wang, Wenting Li, Ping Wang. Measuring Two-Factor Authentication Schemes for Real-Time Data Access in Industrial Wireless Sensor Networks// Industrial Informatics IEEE Transactions. – 2018. – Vol.14, № 9. – P. 4081-4092. (дата обращения: 10.13.2024)
3. Willis, Nathan. FreeOTP multi-factor authentication. [Online]. Available: https://lwn.net/Articles/581086 (дата обращения: 02.13.2024)
4. Бизнеске арналған екі факторлы аутентификация шешімдері.[Онлайн]. Қолжетімді: https://cloudnetworks.ru/analitika/vybor-dvuhfaktornoj-autentifikatsii-2fa/. (қаралған күні 19.03.2024)

ӘОЖ 004.056

“BAGALAIYQ” ПЛАТФОРМАСЫНЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІ

Жемісбек Қапура
Hapura_10@mail.ru
Л.Н. Гумилев атындағы ЕҰУ Ақпараттық қауіпсіздік мамандығының
1 курс магистранты, Астана, Қазақстан
Ғылыми жетекшісі – А.С. Баегизова

Аннотация: Мақалада білім алушылар мен педагогикалық кадрлар арасындағы өзара іс-қимылды жақсартуға, сондай-ақ білім беру ресурстарының сапасы мен қолжетімділігін арттыруға арналған “Bagalaiyq” платформасының ақпараттық қауіпсіздігі қарастырылады. Осы жүйе шеңберінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі шараларға ерекше