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

операций, компании должны усилить свои протоколы проверки и подтверждения личности, особенно при выполнении финансовых операций [5,6].

После обсуждения масштаба проблемы и рассмотрения методов социальной инженерии необходимо перейти к конкретным стратегиям, которые могут помочь в снижении рисков, связанных с человеческим фактором. Важным аспектом является разработка комплексной стратегии кибербезопасности, которая включает в себя как технические решения, так и меры по повышению осведомленности сотрудников.

Во-первых, необходимо проводить регулярные обучающие программы и тренинги для всех сотрудников, чтобы повысить их осведомленность о рисках кибербезопасности и о том, как их минимизировать. Это включает в себя обучение распознаванию фишинговых и других мошеннических сообщений, а также правильному поведению при обнаружении подозрительной активности.

Во-вторых, внедрение технических средств защиты, таких как двухфакторная аутентификация и автоматическое обновление программного обеспечения, может существенно снизить вероятность успешных атак. Также важно регулярно проводить аудиты безопасности и тестирование на проникновение, чтобы выявлять и устранять уязвимости.

В-третьих, создание культуры безопасности внутри организации, где каждый сотрудник понимает свою роль в обеспечении кибербезопасности и поощряется к ответственному отношению к информационной безопасности, является критически важным для минимизации человеческого фактора.

Из всего вышесказанного следует, что человеческий фактор играет центральную роль в кибербезопасности. Несмотря на внедрение технологических средств защиты, без образования и повышения осведомленности сотрудников угрозы остаются высокими. Методы социальной инженерии, особенно фишинг и BEC, демонстрируют, что злоумышленники активно эксплуатируют человеческие ошибки для достижения своих целей. Тем не менее, через комплексные стратегии, объединяющие образование, технические меры и корпоративную культуру безопасности, можно значительно снизить риски, связанные с человеческим фактором. Создание безопасной рабочей среды требует постоянных усилий и сотрудничества на всех уровнях организации.

Список использованных источников

1. Verizon Data Breach Investigations Report, 2023. URL: https://www.verizon.com/business/resources/reports/dbir/

2. Тренды фишинговых атак на организации в 2022–2023 годах// Positive technologies, 2024. URL: https://www.ptsecurity.com/ru-ru/research/analytics/phishing-attacks-on-organizations-in-2022-2023/

3. Phishing Activity Trends Reports// Anti-Phishing Working Group, 2024. URL: https://apwg.org/trendsreports/

4. Deepen Desai, Rohit Hedge, Emily Laufer, Jim Wang 2023 Phishing Report//Zscaler, 2023. URL: https://www.zscaler.com/blogs/security-research/2023-phishing-report-reveals-47-2-surge-phishing-attacks-last-year#article

5. Operating System Security// OWASP, 2021. URL: https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A6-Security_Misconfiguration

6. Information Technology Laboratory//National Vulnerability Database. URL: https://nvd.nist.gov/

ӘОЖ 004.056.5

БІЛІМ БЕРУ ОРТАСЫНДА HONEYPOT ҚОЛДАНУ: КИБЕРҚАУІПСІЗДІКТІ АРТТЫРУ ЖӘНЕ СТУДЕНТТЕРДІ ОҚЫТУ МҮМКІНДІКТЕРІ

Киянбекова Адина Серикқызы
Kianbekovaadina1@gmail.com

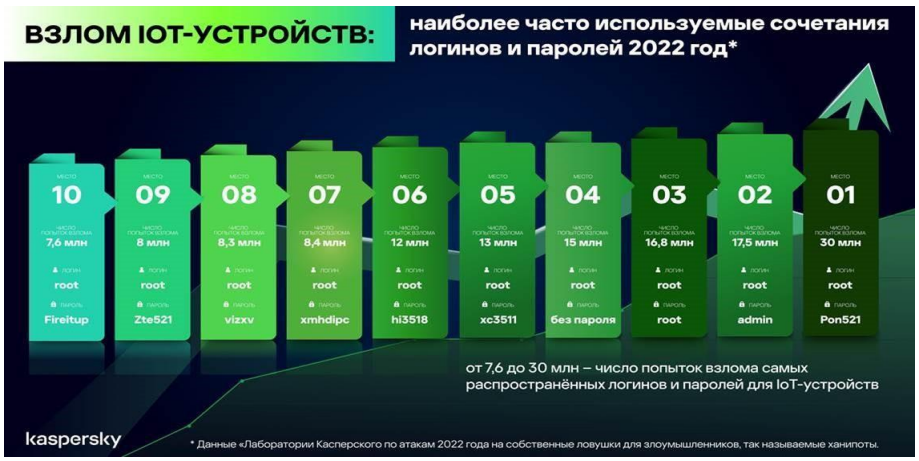
Л.Н.Гумилев атындағы ЕҰУ, «Ақпараттық технологиялар» факультетінің 4-курс студенті, Астана, Қазақстан
Ғылыми жетекшісі – «Ақпараттық қауіпсіздік» кафедрасының аға оқытушысы Г.И.Аймичева

Қазақстан Республикасының цифрлық трансформация, ақпараттық-коммуникациялық технологиялар және киберқауіпсіздік саласын дамытудың 2023 - 2029 жылдарға арналған тұжырымдамасын және "Қазақстанның Киберқалқаны" тұжырымдамасын іске асырудың барлық кезеңінде Киберқауіпсіздік бойынша белгілі бір нәтижелерге қол жеткізілді. Атап айтқанда, сапалы кәсіби қызметтер нарығы құрылды, ақпараттық қауіпсіздік жүйелері мамандығы бойынша білім беру гранттары ұлғайтылды, киберқауіпсіздік мәдениеті артты және т.б.

Қазіргі әлемде ақпараттық қауіпсіздік, ақпараттық жүйелер мен цифрландыру процестері үнемі дамып келеді. Жыл сайын олар жай ғана бір орында тұрмайды, керісінше белсенді дамып, жаңа заман талаптарына тез бейімделеді. Біз үздіксіз даму мен жетілдіруді қажет ететін жаңа қауіптер мен қиындықтарға тап боламыз. Киберқауіпсіздік саласындағы қауіптердің өсуі, шабуылдардың жаңа түрлерінің және зиянды бағдарламалардың әртүрлі түрлерінің пайда болуы бізге ақпараттық ресурстарды қорғауды жақсарту бойынша тұрақты міндеттер қояды. Ақпараттық технологиялар саласындағы зерттеулер тоқтамайтынын да ескеру қажет. АТ әлемінде жыл сайын жаңа аспектілер мен мүмкіндіктер ашылады, бұл бізге біліміміздің байытуға және деректер мен ақпараттық жүйелерді тиімді қорғаудың жаңа жолдарын табуға мүмкіндік береді.

Цифрлық трансформациядан туындаған кибершабуылдар қаупінің өсуіне байланысты ұйымдар өз бизнесіне одан әрі зиян келтірмеу үшін киберқауіптерді азайту үшін белсенді шаралар қабылдауы керек. Ақпараттық қауіпсіздік саласының білікті мамандарын жалдау бұл процесте шешуші рөл атқарады, бірақ бұл салада АҚ мамандарының жетіспеушілігі өзекті мәселе болып табылады. Киберқауіпсіздік саласындағы жаңа мамандарды даярлау үшін білім мен кәсіби даярлыққа көп көңіл бөлу қажет. Тиімді киберқауіпсіздік білім беру бағдарламасы заманауи оқу бағдарламасын қамтуы және практикалық тәжірибені қамтамасыз етуі керек. Мақалада осы саладағы білім сапасын жақсарту үшін Honeypot-ты киберқауіпсіздік зертханасының моделі ретінде ұсынылған.

Honeypots білім беру ортасында киберқауіпсіздік қатерлерін зерттеу және қауіпсіздік шараларын күшейту үшін құнды құрал бола алады, өйткені бұл құрал шабуылдаушылардың тактикасы мен мотивациясын түсінуге мүмкіндік беретін және олардың назарын аудару және алдау қабілеті болып саналады. Honeypots қауіпсіздік және SIEM-жүйелерімен (оқиғалар туралы ақпаратты басқару) салыстырғанда тек белгілі бір аспектілерде ғана тиімді. Honeypots SIEM-жүйелерін толықтыра алады, алайда толығымен алмастыра алмайды [4]. Олар жаңа зиянды бағдарламалар, жаңа шабуыл түрлері туралы ақпаратты жинауға және ақпараттық қауіпсіздік оқиғаларының мінез-құлқын жоғары дәлдікпен бақылауға мүмкіндік береді [6]. Сонымен қатар, жемдер журналдардың егжей-тегжейлі есептерін жасайды, бірақ оларда Endpoint Detection and Response (EDR) және SIEM-технологияларымен үйлесімділік болмауы мүмкін [3] . Сонымен қатар, алаяқтарды SIEM жүйелерімен бірге шабуылдар туралы соңғы ақпаратты алу үшін пайдалануға болады, бұл көп деңгейлі қауіпсіздік архитектурасына ықпал етеді [7]. Мысалы, "Касперский зертханасы" статистикасына сәйкес, IoT-құрылғылар мен қызметтерді бұзу үшін жиі қолданылатын логиндер мен парольдердің тіркелімдері суретте көрсетілген. Бұл суретте Касперский Зертханасының 2022 жылғы көрсеткіші бойынша Honeypot арқылы анықталған шабуылдары туралы мәліметтер келтірілген (1-сурет).

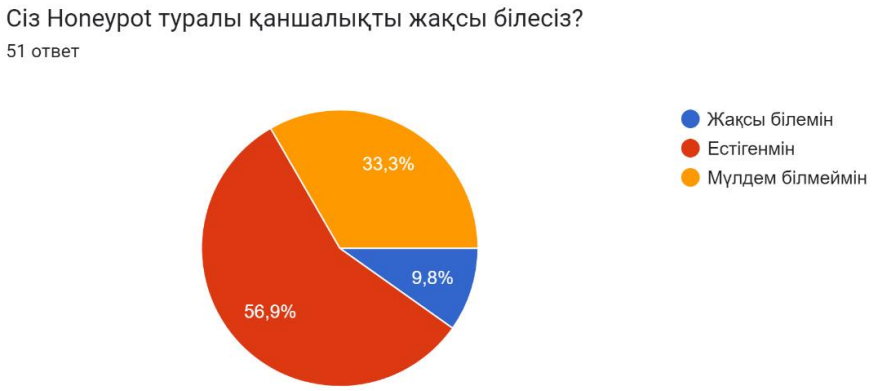


1-сурет. Касперский Зертханасының зерттеуі бойынша Honeypot арқылы IoT-құрылғыларға жасалған шабуыл кезіндегі ең көп қолданылатын логин мен құпия сөздер сипаттамасы [8].

Суретте root және admin құпия сөздері бұзу әрекеттері кезінде жиі қолданылатындығы және Cowrie Honeypot-боты журналының көмегімен echo және uname командалары танымал екенін түсінуге болады. Бұл ақпарат ақпараттық қауіпсіздік саласындағы оқытушылар мен студенттерге құнды тәжірибе береді.

Екінші жағынан, SIEM-жүйелері ақпараттық жүйелер мен деректерге қатысты қауіптерді нақты уақыт режимінде бақылау үшін қажет, бұл ақпараттық қауіпсіздікті қорғау құралдарын қамтамасыз етеді [5]. Олар интрузияны анықтау жүйелері, нөлдік осалдығы бар зиянды бағдарлама детекторлары және аномалия детекторлары сияқты әртүрлі құрамдас бөліктермен өзара байланысты, бұл олардың жұмыс кезінде бақылау жүйелеріндегі маңыздылығын көрсетеді [1]. Дегенмен, Honeypot жүйелерді техникалық қызмет көрсетуден бас тарту, DoS-шабуылдарынан Advanced Persistent Threats (APT) шабуылдарына дейін әртүрлі шабуылдардан қорғау үшін сәтті қолданылатынын атап өткен жөн [2]. Қорытындылай келе, SIEM жүйелері нақты уақыттағы бақылау және ақпараттық қауіпсіздікті қорғау үшін өте маңызды болғанымен, жемдер анықтау тиімділігін арттыру, жаңа зиянды бағдарламалар туралы ақпаратты жинау және егжей-тегжейлі журнал есептерін қамтамасыз ету тұрғысынан бірегей артықшылықтарды ұсынады. Осылайша, Honeypot-ты SIEM жүйелерімен біріктіру киберқауіпсіздік деңгейін жақсартуға айтарлықтай үлес қоса алады.

Біздің білім ордамыздың Ақпараттық қауіпсіздік жүйелерінің студенттері мен түлектері арасында Киберқауіпсіздікті жақсарту үшін Honeypot пайдалану тақырыбындағы сауалнама өткізілген болатын. Сауалнама қатысушыларына Honeypot технологиясы жайында білімі жайлы, оның артықшылықтары мен кемшіліктерін талдау және Honeypot-ты өз ұйымына енгізу тәжірибесі туралы бірқатар сұрақтар қойылды. Аталған сауалнамада біз үшін АТ инфрақұрылымында Honeypot технологиясын пайдаланудың артықшылықтары мен шектеулерін жақсы түсіну үшін білікті мамандардың пікірі мен тәжірибесін білу маңызды. Сауалнама нәтижелері бойынша көп студенттер мен түлектердің Honeypot туралы жеткілікті білімі жоқ екенін көрсетеді, бұл жалпы ақпараттық қауіпсіздік мамандарын даярлайтын жоғары оқу орындарының оқыту контекстіндегі мәселе болып саналады (2-сурет).



2-сурет. Сауалнама қатысушыларының жауаптары үзіндісі [9].

Honeypot-тарды білім беру ортасында практика жүзінде қолдану студенттер мен оқытушылар үшін өте пайдалы болуы мүмкін. Бұл құрал арқылы ақпараттық қауіпсіздік ортасындағы шабуылдаушылардың нақты шабуылдары мен тактикасын байқауға және талдауға мүмкіндік береді, бұл ақпараттық қауіпсіздік саласындағы заманауи қауіптерді зерттеудің бірегей мүмкіндігін қамтамасыз етеді. Бұл тәсіл заманауи қауіптер мен тиімді қорғаныс әдістерін терең түсінуді қалыптастыруға ықпал етеді, бұл студенттер мен оқытушылардың киберқауіпсіздік саласындағы құзыреттілік деңгейін арттырады және қауіпсіз оқыту ортасын жасайды.

Жылда цифрлық технологиялар әлемінде жаңа қауіптер мен жаңалықтар ашылуда. Бұл бізді теориялық жүзінде де, практика кезінде де үнемі жетілдіруге, дамуға, жаңа ақпаратарға сай шешім қабылдауға мәжбүр етеді. Яғни біліміміздің кеңейтуге және деректер мен ақпараттық жүйелерді қорғаудың тиімді әдістерін табуға көмектеседі, бұл қауіп-қатерге қарсы күресте алдыңғы қатарда қалуға және цифрлық әлемді сенімді қорғауға мүмкіндік береді. Киберқауіпсіздік қауіптерінің үнемі өсіп келе жатқан күрделілігі, шабуыл әдістері мен зиянды бағдарламалардың әртүрлілігі ақпараттық ресурстардың қауіпсіздігін қамтамасыз ету тәсілдерін үнемі жетілдіруді талап етеді.

Honeypot-тарды білім беру ортасында қолдану туралы шолу мақаласы олардың маңыздылығы мен ақпараттық қауіпсіздік саласындағы студенттер мен оқытушылардың құзыреттілік деңгейін арттыру үшін пайдалану перспективаларын көрсетеді. Мақаланың бірінші бөлімінде нақты желілік ресурстарды имитациялауға және ықтимал зиянкестердің әрекеттерін талдауға мүмкіндік беретін Honeypot-тардың негізгі тұжырымдамалары мен принциптері қарастырылды. Содан кейін Honeypot-тардың қазіргі киберқауіптерден қорғану құралы ретіндегі тиімділігін көрсететін Касперский Зертханасының зерттеу нәтижелері ұсынылды. Мақала соңында киберқауіпсіздік саласындағы мамандарды даярлаудың жоғары деңгейін қамтамасыз ету және қауіпсіз цифрлық ортаны құру үшін ЖОО-ның білім беру бағдарламаларына хонипоттарды енгізу қажеттілігін көрсететін сауалнама нәтижелері ұсынылды.

Пайдаланылған әдебиеттер

1. Фурнарис, А., Димопулос, К., Лампропулос, К. Және Куфопавлу, О. (2020). Аномалияны анықтау маңызды инфрақұрылымның ескірген құрылғыларына арналған сенімді аппараттық сенсорлар. Датчиктер, 20 (11), 3092. https://doi.org/10.3390/s20113092

2. Ли, С., Чо, К. Және Ким, С. (2022). Кәдімгі серверлерді бал құмыралары ретінде жасыру керек пе?.. https://doi.org/10.48550/arxiv.2210.17399

3. Сетианто, Ф. (2021). Gpt-2c: cowrie honeypot журналдарына арналған gpt-2 талдағышы.. https://doi.org/10.48550/arxiv.2109.06595

4. Спирос, А., Папутсис, А., Корицас, И., Менгидис, Н., Илиу, С., Кавальерос, Д., ... Және Компатиарис, И. (2022). Киберқауіптер туралы ақпаратты үнемі байыту бағытында: бал құмыралары туралы мәліметтер жиынтығын зерттеу.. https://doi.org/10.1109/csr54599.2022.9850295

5. Суросо, Дж.және Прастя, С. (2020). Жоғары оқу орындарында siem және honeypot бар киберқауіпсіздік жүйесі. Iop Конференция Сериясы Материалтану және Инженерия, 874(1), 012008. https://doi.org/10.1088/1757-899x/874/1/012008

6. Vrable, M., Ma, J., Chen, J., Moore, D., Vandekieft, E., Snoeren, A., ... & Savage, S. (2005). Потемкин виртуалды бал фермасындағы ауқымдылық, адалдық және ұстамдылық. Acm Sigops Операциялық Жүйелеріне Шолу, 39 (5), 148-162. https://doi.org/10.1145/1095809.1095825

7. Вебер, С., Штайн, С., Пилгерманн, М. Және Шрейдер, Т. (2023). Медициналық киберфизикалық жүйелер үшін шабуылдарды анықтау-әдебиеттерге жүйелі шолу. Ieee Қол Жетімділігі, 11, 41796-41815. https://doi.org/10.1109/access.2023.3270225

8. https://www.kaspersky.ru/about/press-releases/2022_klyuchi-dlya-umnyh-ustrojstv-kakie-sochetaniya-loginov-i-parolej-chashe-vsego-vvodyat-zloumyshlenniki

9. https://docs.google.com/forms/d/e/1FAIpQLSfeDQ-6S8_4b7XAtfWvdfpC1BF5F0C524Mw_wtajGsZlPf5Mw/viewform?usp=sharing

ӘОЖ 004.056

ҚАУІПСІЗДІКТІ АРТТЫРУ ӘДІСТЕРІ: КІЛТ ҰЗЫНДЫҒЫН ҰЛҒАЙТУ ЖӘНЕ ХЭШ ФУНКЦИЯЛАРЫН ПАЙДАЛАНУ

Қалыбек Иманғали Рахымжанұлы
imangalikalybek@gmail.com
Л.Н.Гумилев атындағы ЕҰУ, «Ақпараттық қауіпсіздік жүйелері»
білім беру бағдарламасының 1-ші курс магистранты, Астана, Қазақстан
Ғылыми жетекші – Жаркимбекова А.Т.

Аңдатпа. Зерттеу жұмысында криптографиялық қорғаудың екі негізгі аспектісін жақсарту арқылы киберқауіпсіздікті арттыру мәселелері қарастырылады: кілт ұзындығын ұлғайту және хэш функцияларын пайдалану. Үнемі дамып келе жатқан киберқауіптер мен шабуылдаушылардың есептеу қуатының артуы жағдайында авторлар сенімді хэш-функцияларды қолданумен бірге криптографиялық алгоритмдердегі кілт ұзындығын ұлғайтуды ұсынады. Мақалада осы әдістердің тиімділігі талданады және заманауи ақпараттық ортада киберқауіпсіздік деңгейін арттыру үшін оларды қолдану бойынша практикалық ұсыныстар ұсынылады. Зерттеу нәтижесінде осы әдістердің ықтимал қауіптері мен артықшылықтары анықталды, бұл мақаланы ақпараттық қауіпсіздік саласындағы мамандар мен барлық мүдделі тұлғалар үшін өзекті етеді.

Кілт сөздер: ақпараттық қауіпсіздік, шифрлау, криптография, хэш-функция, киберқауіпсіздік, криптографиялық алгоритм.

1. Кіріспе

Қазіргі уақытта цифрлық әлем ақпаратпен тығыз байланысты және желіге қосылған кеңістікті білдіреді. Дегенмен, интернет-технологиялардың өсуімен және цифрлық деректер көлемінің ұлғаюымен киберқауіпсіздік тәуекелдері де артады. Деректер мен жеке ақпаратты қорғаудың тиімді әдістерін қажет ететін ұйымдар мен жеке тұлғаларға технологиялар өзгерген сайын көбірек қауіп төндіреді. Бұл тұрғыда криптография деректердің құпиялылығын, тұтастығын және аутентификациясын қамтамасыз ету құралдарын қамтамасыз ету арқылы негізгі рөл атқарады. Дегенмен, шабуылдың жаңа әдістерінің пайда болуымен және заманауи компьютерлердің есептеу қуатының артуына байланысты бұрын қауіпсіз болып көрінген криптографиялық алгоритмдер уақыт өте келе осал болуы мүмкін. Зерттеу жұмысында біз киберқауіпсіздікті жақсартудың екі маңызды аспектісіне тоқталамыз: кілт ұзындығын ұлғайту