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

– Қауіпсіздік және оқиғалар туралы ақпаратты басқару (SIEM): SIEM шешімдері нақты уақыт режимінде қауіпсіздік оқиғаларын ұсынуды қамтамасыз ететін және оқиғаларға жылдам жауап беруді қамтамасыз ететін АТ инфрақұрылымы бойынша әртүрлі ресурстардың белсенділігін біріктіреді және талдайды.

“Білім алушыларға арналған “Bagalaiyq” жүйесінің ақпараттық қауіпсіздігін қамтамасыз ету” ақпараттық қауіпсіздік шараларын қатаң сақтай отырып, заманауи технологияларды білім беру процесіне біріктірудің маңыздылығын атап көрсетеді. “Bagalaiyq” жүйесі оқушылар мен педагогтарға сапалы ресурстар мен құралдарды ұсына алатын, осылайша білім деңгейін арттыруға және сыни ойлау дағдыларын дамытуға ықпал ететін білім беру саласындағы қуатты құрал болып табылады [4].

“Bagalaiyq”-те ақпараттық қауіпсіздікті қамтамасыз ету жүйені сыртқы және ішкі қауіптерден қорғап қана қоймай, пайдаланушылардың платформаға деген сенімін нығайтады. Деректерді шифрлауды, аутентификацияны және кіруді басқаруды, сондай-ақ қауіпсіздік бойынша тұрақты аудиттер мен тренингтерді қоса алғанда, қауіпсіздік шаралары дербес және оқу деректерін сенімді қорғауды қамтамасыз етеді. Осылайша, “Bagalaiyq” білім беру жүйесін әзірлеу және қолдау сапалы және қауіпсіз білім беру процесін қамтамасыз ету үшін маңызды міндет болып қала береді.

Қолданылған әдебиеттер тізімі

1. Иванов И.И., Петров П.П. Кибербезопасность в образовательных учреждениях. М.: Издательство "Наука", 2020.
2. Смирнов А.А., Лебедев К.С. Методы и средства обеспечения информационной безопасности в компьютерных системах. СПб.: Издательство "Лань", 2019.
3. Михайлов М.М., Зайцев Д.Н. Современные технологии защиты информации. Новосибирск: Издательство "Научная книга", 2021.
4. Горбунова Л.В., Чернышова Т.В. Компьютерная безопасность и защита информации в образовательных системах. Екатеринбург: Издательство Уральского университета, 2018.

УДК 004.056.53

ЧЕЛОВЕЧЕСКИЙ ФАКТОР КАК КЛЮЧЕВОЙ ЭЛЕМЕНТ В УЯЗВИМОСТИ ОПЕРАЦИОННЫХ СИСТЕМ: АНАЛИЗ И СТРАТЕГИИ УМЕНЬШЕНИЯ РИСКОВ

Жұмашев Санжар Маратқалиұлы
zhumashevsanzhar@gmail.com
Магистрант 2-ого курса ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – к.ф.-м.н., доцент Сауханова Ж.С.

Аннотация: Данная обзорная статья посвящена проблеме влияния человеческого фактора на уровень безопасности операционных систем. В ней поясняется актуальность и важность рассматриваемой темы, приводятся примеры уязвимости из практики и подтверждаются результатами статистических данных. Кроме того, автором предлагаются рекомендации для устранения уязвимостей.

Ключевые слова: пользователь, операционная система, человеческий фактор, кибербезопасность, информационные технологии, система безопасности, уязвимость.

В современном мире, где операционные системы становятся основой кибербезопасности, человеческий фактор играет решающую роль в обеспечении их безопасности. Эта статья исследует влияние пользовательского взаимодействия и человеческих ошибок на безопасность операционных систем.

Основываясь на данных Verizon 2023 Data Breach Investigations Report, можно утверждать, что человеческий фактор продолжает играть значительную роль в кибербезопасности, влияя на 74 % всех инцидентов. Это означает, что большинство

нарушений безопасности можно отнести к действиям или промахам пользователей, а не к техническим недостаткам операционных систем или сетевой инфраструктуры [1].

Человеческий фактор включает в себя широкий спектр ошибок: от простых просчетов, таких как ненадлежащее обращение с паролями, до более сложных видов социальной инженерии, таких как фишинг.

Фишинг – это одна из разновидностей интернет-мошенничества, целью которого является получение конфиденциальной информации, и он остается одной из наиболее распространенных методик, поскольку атакующие постоянно совершенствуют свои тактики, делая сообщения всё более убедительными и трудноотличимыми от легитимных.

В 2023 году наблюдается заметное увеличение активности фишинговых атак, особенно с использованием социальной инженерии. Примерно 43% всех успешных атак на организации были совершены с использованием методов социальной инженерии, преимущественно через электронную почту, СМС, социальные сети и мессенджеры. Такие атаки часто направлены на сотрудников, контролирующих крупные суммы денег, и могут включать в себя не только кражу учетных данных, но и последующие многоэтапные переводы денежных средств на контролируемые злоумышленниками счета [2]. Согласно отчетам Anti-Phishing Working Group, в 2023 году было зарегистрировано почти пять миллионов фишинговых атак, что делает этот год рекордным по количеству таких инцидентов. Во второй половине года атаки против социальных медиа платформ резко возросли, составив 42,8 % от всех фишинговых атак [3].

Другими наиболее часто атакуемыми отраслями стали образование, финансы и розничная торговля. В частности, образовательная сфера столкнулась с увеличением числа атак на 576 %, тогда как в розничной и оптовой торговле наблюдалось снижение на 67%. [4]. Важно отметить, что руководители компаний часто становятся целями для киберпреступников из-за доступа к конфиденциальной информации и более слабых протоколов безопасности. Это подчеркивает необходимость усиления мер безопасности для всех уровней сотрудников, особенно для тех, кто имеет доступ к критически важной информации. Опираясь на вышеперечисленную статистику необходимо сформировать понимание масштабов проблемы и идентификации основных человеческих факторов, влияющих на безопасность операционных систем и данных. Знание этих факторов является первым шагом к разработке эффективных стратегий снижения рисков и повышения уровня кибербезопасности

Продолжая анализ человеческого фактора, особое внимание следует уделить противостоянию пользователей методам социальной инженерии, которые используются злоумышленниками для эксплуатации человеческих ошибок. Социальная инженерия охватывает широкий спектр действий, направленных на манипулирование людьми для получения конфиденциальной информации или доступа к системам. По этой причине пользователям, которые могут владеть конфиденциальной информацией, в которой заинтересованы злоумышленники, необходимо владеть базовыми знаниями в области информационной безопасности, в частности социальной инженерии. Осведомленность пользователей позволит сократить случаи овладевания всей необходимой информацией злоумышленниками, которая будет использована для проведения дальнейших атак. Стоит отметить, что атаки, которые следуют после успешного проведения социальной инженерии, несут в себе наибольшую угрозу, поскольку большинство предпринятых мер по выстраиванию системы безопасности могут не сработать в критически важный момент.

Рост фишинговых атак и других форм социальной инженерии, особенно в частой практике внедрения формата удаленной работы, подчеркивает важность осведомленности и образования сотрудников. Обучение должно включать распознавание подозрительных сообщений, понимание рисков некритического отношения к информационной безопасности и знание действий при обнаружении потенциальной угрозы. Кроме того, с ростом тактик, используемых в бизнес-электронных компрометациях (BEC), где злоумышленники имитируют сотрудников высшего звена для совершения мошеннических финансовых

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