https://doi.org/10.53656/str2023-5s-7-onl

Research Results
Резултати от научни изследвания

ОНЛАЙН ТРЕНИРОВКИ И КИБЕРСИГУРНОСТ: ПОТЕНЦИАЛНИ ЗАПЛАХИ И ПРЕВЕНЦИЯ

Гл. ас. д-р Диляна Зайкова
Национална спортна академия „Васил Левски“
Петър Йорданов
Военна академия „Георги С. Раковски“

Резюме. В съвременния цифров свят онлайн комуникацията придоби широка популярност като ефективен и лесно достъпен начин за поддържане дейността на редица сфери от живота, в това число и провеждането на онлайн тренировки с фитнес инструктори. Въпреки ползите, свързани с онлайн тренировките, неизбежно се появяват предизвикателства в областта на киберсигурността, които изискват сериозно внимание и превантивни мерки. Целта на проучването е да се анализира ефективността на настоящите механизми и политики за онлайн сигурност и да се идентифицират потенциални заплахи, свързани с онлайн тренировките и киберсигурността. Най-висока ефективност се постига в защитата на личните данни на потребителите и предотвратяването на хакерски атаки. Водещите потенциални заплахи са фишинг атаки, злоупотреба с лични данни и инсталиране на зловреден софтуер. Най-често използваните механизми постигат оптимална киберсигурност, но непрекъснатите онлайн заплахи изискват повишено внимание и от страна на потребителите. Използването на силни и уникални пароли за всички онлайн акаунти, актуализиране на софтуера на устройствата, използването на двуфакторна автентикация и създаването на резервни копия, ще повишат ефективността на онлайн защитата.

Ключови думи: онлайн фитнес тренировки; киберсигурност; защита на лични данни; хакерски атаки; фишинг

Въведение

В съвременния цифров свят онлайн комуникацията придоби широка популярност като ефективен и лесно достъпен начин за поддържане дейността на редица сфери от живота, в това число и провеждането на онлайн тренировки с фитнес инструктори. Прогнозите са онлайн фитнес пазарът да достигне невероятни размери през следващите години. През 2022 г. той е оценен на стойност над 14.9 милиарда щатски долара и се очаква да расте със скорост от

над 32.7% годишно до 2032 г., достигайки 250.7 милиарда щатски долара през 2032 г. (Mayabrahmma et al. 2023).

Онлайн фитнес тренировките придобиха значителна популярност и се превърнаха в предпочитан метод за достъп до обучение и физическа активност, предлагайки гъвкавост, удобство и глобален достъп, което ги прави изключително атрактивни за широката аудитория (Better 2020; Mayabrahmma et al. 2023). Този вид тренировки предоставят възможност на потребителите за достъп до платформата в удобно за тях време, избор на треньор и тренировъчни програми, ниво на трудност, участие в индивидуална или колективна тренировка (Mayabrahmma et al. 2023). Те са предпочитан метод на тренировка при хора с ограничено физическо време, хора с физически увреждания (Sharon-David et al. 2020) или различни заболявания (Hansen et al. 2020), домакини, жени в майчинство (Saligheh et al. 2016), хора със затлъстяване (Ball et al. 2000), хора в напреднала възраст (Hong et al. 2018; Baez et al. 2016).

Наред с ползите, свързани с онлайн тренировките, неизбежно се появяват предизвикателства в областта на киберсигурността, които изискват сериозно внимание и превантивни мерки. Тяхното изолиране и актуализиране на механизмите и политиките за киберсигурност ще доведе до създаването на по-сигурна среда за провеждане на онлайн фитнес тренировки и ще повиши доверието на потребителите (Alammari et al. 2022). За запазването на ефективността, сигурността и надеждността на онлайн тренировките като метод за спорт и обучение в дигиталната ера е важно да се внедрят адекватни мерки за сигурност. Тези мерки могат да включват използването на сигурни пароли и двуфакторна автентикация, криптиране на данните и редовни ъпдейти на софтуера (Sebastian 2021).

Цел

Целта на настоящото проучване е да анализира заплахите и предизвикателствата, свързани с онлайн тренировките и киберсигурността, и да предложи решения и препоръки за подобряване сигурността на данните и информационната среда в контекста на тези тренировки.

Методика

Анализ по ключови думи на научните публикации в Google Scholar, Researchgate, IEEE Xplore, Scopus и др. относно актуалните механизми и политики за киберсигурност, както и предизвикателствата, свързани с провеждането на онлайн фитнес тренировки. Извличане на ключови концепции, методи и практики, свързани с киберсигурността. Предоставяне на препоръки за сигурност и стандарти, обучение на потребителите, създаване на осведомителни кампании и насърчаване на отговорното поведение в онлайн средата.

Резултати

Чрез анализ на релевантната литература обобщихме основните предизвикателства и заплахи, които възникват при използването на онлайн платформите за фитнес тренировки (фиг.1).

Фигура 1. Предизвикателства и заплахи

Прегледахме актуалните мерки и решения и проучихме текущото състояние на киберсигурността при провеждане на онлайн фитнес тренировки (табл. 1).

Таблица 1. Мерки за киберсигурност при платформите за онлайн фитнес тренировки

Мерки за киберсигурност
1. Изследване архитектурата на системите Анализиране и проектиране структурата и функционалността на софтуерни или хардуерни системи: подходящи компоненти, протоколи, алгоритми и интерфейси.
2. Автоматизирани системи за откриване на атаки Интелектуална аналитика и мониторинг с цел разпознаване на необичайна активност и предотвратяването на кибератаки в реално време.
3. Мултифакторна автентикация (MFA) Потребителите предоставят повече от една форма на идентификация, като парола и SMS код или биометрични данни, с цел увеличаване на сигурността и затрудняване на неоторизиран достъп до тренировъчните сесии.

4. Редовни актуализации на софтуера Актуализации и пачове за предотвратяване на експлоатация на известни уязвимости.
5. Криптирането на данни и защита на личната информация Преобразуване на информацията в код, който може да бъде разчетен само с помощта на специален ключ. Целта на криптирането е да предпази данните от неоторизиран достъп или злоупотреба.
6. Firewalls и Intrusion Detection/Prevention Systems (IDS/IPS) Тези технологии контролират и мониторират трафика в мрежата, за да идентифицират вредни активности и да предотвратяват неоторизирани достъпи.
7. Сигурност на приложенията Защита срещу уязвимости като SQL инжекции и кръстосани сайтове.
8. Разделяне на правата на достъп Потребителите и администраторите следва да имат само правата, които са им необходими, за да намалят риска от злоупотреби.
9. Резервни копия Водещи са след претърпени атаки или събития с цел възстановяване на данните.
10. Облачни решения и сигурност на сървъра Подпомагат предотвратяването на множество заплахи за киберсигурността при провеждането на онлайн фитнес тренировки.
11. Сигурност при комуникацията Защита на сигурността при комуникацията между клиентите и сървъра чрез протоколи за шифроване (например HTTPS).

Дискусия

Онлайн средата е изправена пред заплахи от злонамерени софтуери (малуер) като вируси, червеи, троянски коне, шпионски софтуери, рекламни софтуери и др. Щетите, причинени от вирус, който е заразил домашен компютър или корпоративна мрежа, могат да бъдат различни – от незначително увеличение на изходящия трафик до пълен срив на мрежата или загуба на критични данни. Най-разпространени злонамерени софтуери са рисковият и рекламният софтуер поради факта, че потребителите използват личните си лаптопи или други смарт устройства за участие в онлайн тренировките. Щетите, които тези софтуери могат да нанесат, са повреда на хардуера, загуба или кражба на данни, нарушаване работата на устройството (Chen, He 2013; Sebastian 2021; Szczepaniuk, Szczepaniuk 2022).

Кражбата на данни е един от водещите проблеми за онлайн потребителите. Често се използват фалшиви портали под формата на източник за получаване на разрешение за достъп до устройството и информация за пароли и лични данни (Sebastian 2021; Szczepaniuk, Szczepaniuk 2022).

Атаката за отказ на услуга (DDoS) цели изключване на устройствата или мрежата, като ги прави недостъпни за потребителите (Sebastian 2021), особено

при използване на приложения за видеоконференции като Zoom (Raza, 2020). DoS атаките трябва да се очакват при онлайн потребителите, тъй като обикновено те имат по-малък контрол върху сигурността на устройствата си и мрежите (Sebastian 2020).

Нелегитимният достъп до тренировъчни сесии е проблем, който може да засегне киберсигурността и личната информация на потребителите. Онлайн платформите за провеждане на тренировки трябва да са защитени с парола, шифроване и други мерки за сигурност с цел предотвратяване на наблюдение от нежелани лица, прекъсване на тренировъчната сесия и кражба на лични данни. Специалистите в областта на киберсигурността препоръчват да се избягва споделянето на лична информация или връзки към тренировките в публичните или социалните медии (Szczepaniuk, Szczepaniuk 2022).

Уязвимости в сигурността на платформите са слабости, които могат да бъдат използвани от злонамерени хора или програми, за да нападнат или компрометират системи или данни. Те могат да бъдат предизвикани от грешки в кода или конфигурациите на платформите, които се използват (Szczepaniuk, Szczepaniuk 2022).

Социалният инженеринг е метод за хакване или шпиониране, който използва манипулация или измама, за да накара хората да разкрият конфиденциална информация или да предоставят достъп до своите системи или акаунти. Социалният инженеринг се основава на използването на човешките слабости, като доверие, любопитство, страх или желание. Социалният инженеринг може да се извършва по различни начини, като физически достъп, имейл фишинг, телефонни обаждания, съобщения или други средства за комуникация (Koyun 2017).

Видео уроците и учебните материали се съхраняват безопасно, за да се предотврати неразрешеното им копиране или разпространение. Използването на сигурни връзки и канали за комуникация между участниците и инструкторите гарантира поверителността и неприкосновеността на съобщенията (Szczepaniuk, Szczepaniuk 2022).

Онлайн тренировъчните платформи често събират лични данни на участниците. Защитата на тези данни от неразрешен достъп е критична. Инвестирането в сигурни платформи и мерки за защита на личните данни на участниците гарантира поверителността и неприкосновеността на техните лични информации (Chen, He 2013).

Предизвикателствата в областта на киберсигурността при онлайн тренировките са много и от различно естество. За справяне с тях препоръчваме образователните институции и организаторите на онлайн тренировки да разработят и внедрят допълнителни мерки за онлайн защита.

– **Сътрудничество със специалисти по киберсигурност,** експертно мнение и съвети относно най-добрите практики в областта на киберсигурността;

одити на сигурността, пенетрационни тестове и други форми на проверка на сигурността.

– **Съвместимост със законодателство и регулации:** внедряването на сигурни мерки за защита на данните и спазването на законодателството допринася за съответствието със законовите изисквания и предпазва участниците от неправомерно обработване на техните лични данни.

– **Осведоменост и обучение на потребителите:** обучението на потребителите относно основните принципи на киберсигурността намалява вероятността от извършване на грешки, които биха могли да доведат до компрометиране на сигурността.

– **Доверие и репутация:** осигуряването на сигурност и защита на данните на участниците в онлайн тренировките ще подобри качеството на предлаганото обучение и тренировки и ще привлече повече потребители.

Заключение

За да се гарантира сигурността при провеждане на онлайн фитнес тренировки, е важно да се инвестира в сигурни платформи, обучение на потребителите, редовна поддръжка и мониторинг на системите. Използването на криптиране на данни, защита от фишинг атаки и сигурна връзка също са важни аспекти за подобряване на киберсигурността. Систематичните проверки и контрол при онлайн фитнес тренировките изразяват важен аспект на киберсигурността. Те осигуряват защита на личните данни и предотвратяват възможни киберзаплахи. Редовните проверки подобряват надеждността на платформата, предотвратяват злоупотреби и осигуряват защитеността на плащанията. Подобен подход, включващ и актуализации на софтуера, гарантира цялостна киберсигурност и създава доверие сред потребителите.

REFERENCES

ALAMMARI, A.; SOHAIB, O.; YOUNES, S., 2022. Developing and evaluating cybersecurity competencies for students in computing programs. *PeerJ Comput Sci*. Vol. 8; article e827. DOI: 10.7717/peerj-cs.827.

BAEZ, M.; FAR, I. K.; IBARRA, F.; FERRON, M.; DIDINO, D. & CASATI, F., 2016. Effects of online group exercises for older adults on physical, psychological, and social wellbeing: *A pilot trial. Peer J*, vol. 5, no. 4, pp. 1 – 29. https://doi.org/10.7717/peerj.3150.

BALL, K.; CRAWFORD, D. & OWEN, N., 2000. Too fat to exercise? Obesity as a barrier to physical activity. *Australian and New Zealand Journal of Public Health*, vol. 24, no. 3, pp. 331 – 333.

BETTER, 2020. *Top excuses people use for not going to the gym*. [Retrieved from https://www.better.org.uk/content_pages/top-gym-excuses].

CHEN, Y., & HE, W., 2013. Security Risks and Protection in Online Learning: A Survey. *IRRODL*, vol. 14, issue 5, pp. 108 – 127.

HANSEN, H.; BIELER, T.; BEYER, N.; KALLEMOSE, T.; WILCKE, J.T.; ØSTERGAARD, L.M.; ANDEASSEN, H.F.; MARTINEZ, G.; LAVESEN, M.; FRØLICH, A. & GODTFREDSEN, N. S., 2020. Supervised pulmonary tele-rehabilitation versus pulmonary rehabilitation in severe COPD: A randomized multicenter trial. *Thorax*, vol. 75, no. 5, pp. 413 – 421.

HONG, J.; KONG, H. J. & YOON, H. J., 2018. Web-based telepresence exercise program for community-dwelling elderly women with a high risk of falling: Randomized control trial. *Journal of Medical Internet Research mHealth & uHealth*, vol. 6; no. 5, article e132. https://doi.org/10.2196/mhealth.9563.

KOYUN, A., 2017. Social Engineering Attacks, *JMEST*, vol. 4, no. 6, pp. 7533 – 7538.

MAYABRAHMMA, A.; BEESETTY, Y.; SHADAAB, K. & VINEET, K. 2023. *Online/Virtual Fitness Market*, pp. 294, Available from https://www.alliedmarketresearch.com/virtual-online-fitness-market.

RAZA, A., 2020. FBI Says Zoom Video Conference Vulnerable to Attacks, *Koddos Protection*. [Viewed 1 April 2020], Available from https://blog.koddos.net/fbi-says-zoom-video-conference-vulnerable-to-attacks/.

SALIGHEH, M., MCNAMARA, B. & ROONEY, R., 2016. Perceived barriers and enablers of physical activity in postpartum women: a qualitative approach. *BMC Pregnancy Childbirth* vol. 16, pp. 131. https://doi.org/10.1186/s12884-016-0908-x.

SEBASTIAN, G., 2021. The Changing Face of Education: Risk, Security and Process Around Distance Learning. *ISACA Journal*, vol 4, no. 14.

SEBASTIAN, G., 2020. Evolution of the Role of Risk and Controls Team in an ERP Implementation. *International Journal of Mechanical and Production Engineering Research and Development*, vol. 10, no. 3, pp. 15529 – 15532.

SHARON-DAVID, H.; SIEKANSKA, M. & TENENBAUM, G., 2020. Are gyms fit for all? A scoping review of the barriers and facilitators to gym-based exercise participation experienced by people with physical disabilities. *Performance Enhancement & Health*, vol. 9, no. 1, article 100170. DOI: 10.1016/j.peh.2020.100170;

SZCZEPANIUK, E. D., & SZCZEPANIUK, H., 2022. Analysis of cybersecurity competencies: Recommendations for telecommunications policy. *Telecommunications Policy*, Vol. 46, Issue 3. https://doi.org/10.1016/j.telpol.2021.102282.

ONLINE FITNESS TRAINING AND CYBERSECURITY: POTENTIAL THREATS AND PREVENTION

Abstract. In today's digital world, online communication has gained wide popularity as an effective and easy way to maintain the activity of a number of areas of life, including conducting online workouts with fitness instructors. Despite the benefits associated with online training, cybersecurity challenges are inevitably emerging that require serious attention and preventive measures. The aim of the study is to analyze the effectiveness of current online security mechanisms and policies and to identify potential threats related to online training and cybersecurity. The highest efficiency is achieved in protecting users' personal data and preventing hacker attacks. The leading potential threats are phishing attacks, misuse of personal data and malware installation. The most commonly used mechanisms achieve optimal cybersecurity, but continuous online threats require increased attention from users as well. Using strong and unique passwords for all online accounts, updating device software, using two-factor authentication and creating backups will increase the effectiveness of online security.

Keywords: online fitness training; cybersecurity; personal data protection; hacking attacks; phishing

✉ **Dr. Dilyana Zaykova, Assist. Prof.**
ORCID iD: 0000-0003-4696-7463
Department of „Heavy athletics, boxing, fencing and sport for all“
National Sports Academy “Vassil Levski”
E-mail: dilyana.zaykova@nsa.bg

✉ **Petar Yordanov**
ORCID iD: 0000-0003-3860-6019
Faculty of Command and Staff
Rakovski National Defence College
Sofia, Bulgaria