Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра економічної кібернетики

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

Матеріали
наукової онлайн-конференції

(Суми, 07 вересня 2023)

Суми
Сумський державний університет
2023

004.056.5:336(082)
В43

Затверджено Вченою Радою Сумського державного університету (протокол № 2, 14.09.2023)

S62 Виклики кібербезпеки індустрії фінансових послуг: Матеріали наукової онлайн-конференції, Суми, 07 вересня 2023. Збірник матеріалів тез наукової онлайн-конференції / за загальною редакцією доц. Койбічук В.В. – Суми : Сумський державний університет, 2023. – 183 с.

Матеріали наукової онлайн-конференції " Виклики кібербезпеки індустрії фінансових послуг" присвячені пошуку системного вирішення проблем у сфері протидії кібеззагрозам у сфері фінансових послуг, підвищенню рівня кіберзахисту об'єктів критичної інфраструктури.

Видання розраховане на науковців, викладачів, студентів вищих навчальних закладів, аспірантів, докторантів та інших зацікавлених осіб.

004.056.5:336(082)

ЗМІСТ

КІБЕРБЕЗПЕКА БІЗНЕСУ МАЛИХ ТА СЕРЕДНІХ ПІДРПРИЄМСТВ: ДОСВІД ЄС

CYBERSECURITY OF SMALL AND MEDIUM-SIZED ENTERPRISES: EU EXPERIENCE

***Віталія Койбічук**, к.е.н, доцентка*
Сумський державний університет, Україна

З розвитком процесів діджиталізації розвиваються й кіберзагрози й кіберзлочинні схеми, особливо у фінансових системах та індрустрії фінансових послуг, включаючи, але не обмежуючись, послуги інтернет-банкінгу, необанкінгу та грошові перекази, роздрібні платіжні системи, мобільні банківські та платіжні системи, цифрові валюти та інші фінансові послуги. Ці загрози включають крадіжку інформації та коштів клієнтів, відмивання грошей, несанкціоновані перекази та інші зловмисні дії, відмову в обслуговуванні, впровадження шкідливих програм, програм-вимагачів, фішинг, соціальну інженерію та витоки даних. Атаки на фінансові установи можуть мати серйозні ризики для безпеки клієнтів, операцій і фінансів (Kuzmenko et. al, 2021). Тому, надзвичайно важливим для компаній, банків, фінансових установ, підприємств, (всіх соціально-економічних об'єктів) стежити за станом своєї кібербезпеки та мати надійний захист від потенційних атак, а також повинні застосовувати безпечні методи автентифікації клієнтів і шифрування даних, щоб захистити конфіденційні дані клієнтів. Зокрема, Агентство Європейського Союзу з кібербезпеки (ENISA) рекомендує дотримуватися 12 кроків для якісної кібербезпеки ведення бізнесу малими та середніми підприємствами (Cybersecurity guide for SMEs, 2021).

1. Розвивати гарну культуру кібербезпеки: призначити відповідальну особу за організацію кібербезпеки; проводити аудити кібербезпеки; пам'ятати про захист даних.Надійна кібербезпека – запурока сталого розвитку та успіху будь-якого бізнесу. Тому необхідно призначити відповідальну особу, яка повинна забезпечити відповідні ресурси, такі як час від персоналу, придбання програмного забезпечення, послуги і обладнання для кібербезпеки, навчання персоналу та розвиток ефективної політики щодо кібербезпеки. Крім того необхідно мати відкриту підтримку керівництва щодо ініціатив у сфері кібербезпеки, проведення відповідних тренінгів для співробітників та надання чітких, конкретних правил, викладених у політиках кібербезпеки, що регулярно переглядаються та оновлюються. У політиках мають бути прописані наслідки, з якими може зіткнутися працівник, якщо не буде дотримуватимуться політики кібербезпеки. Регулярні аудити повинні проводитися особами, які мають відповідні знання, навички та досвід та не

залежать від щоденних ІТ-операцій. Згідно із Загальним регламентом ЄС щодо захисту даних, будь-які підприємства, фінансові установи, які обробляють або зберігають персональні дані резидентів Європейської економічної зони, повинні забезпечити відповідні засоби контролю безпеки для захисту цих даних. Це гарантує захист інтересів третіх сторін, які працюють від імені відвідного підприємства, та надає їм заходи безпеки.

2. Забезпечити відповідне навчання. Проводити регулярні тренінги з кібербезпеки для всіх співробітників, щоб вони могли розпізнавати різні загрози кібербезпеці та боротися з ними. Ці тренінги мають бути адаптовані для малих підприємств та зосереджені на реальних ситуаціях.

3. Забезпечити ефективне управління третьою стороною. Переконатися, що всі постачальники, особливо ті, хто мають доступ до конфіденційних даних та/або систем, активно керуються та відповідають узгодженим рівням безпеки. В контрактних угодах повинно бути прописано, як постачальники відповідають вимогам безпеки.

4. Розробити план реагування на інциденти. Офіційний план реагування на інциденти має містити чіткі вказівки, ролі та обов'язки, задокументовані для забезпечення своєчасного, професійного та належного реагування на всі інциденти безпеки. Для того, щоб швидко реагувати на загрози безпеці, необхідно досліджувати та аналізувати інструменти, що можуть відстежувати та створювати сповіщення, за умов підозрілих дій або порушення безпеки.

5. Безпечний доступ до систем. Використовувати фразу-пароль, що є набором принаймні трьох випадкових поширених слів, об'єднаних у фразу, яка забезпечує дуже хороше поєднання запам'ятовуваності та безпеки: не використовувати повторно в іншому місці; не діліться з колегами; увімкнути багатофакторну автентифікацію; використовувати спеціальний менеджер паролів. За умов використання типового паролю, рекомендовано робити його довгим, із символами верхнього та нижнього регістру та спеціальними символами. Уникати використання «123», «пароль», особистої інформації, що є відкритому доступі в Інтернеті.

6. Безпека пристроїв. Ключовим кроком у програмі кібербезпеки є забезпечення безпеки пристроїв, якими користуються співробітники (настільні ПК, ноутбуки, планшети чи смартфони), тому необхідно зберігати програмне забезпечення виправленим та оновленим (в ідеалі використовувати централізовану платформу для керування виправленнями). Централізоване кероване антивірусне ПЗ має бути впроваджено на всіх типах пристроїв та підтримуватися в актуальному стані, щоб забезпечити його постійну ефективність. Використовувати ПЗ для блокування електронних листів зі спамом, електронних листів із посиланнями на шкідливі веб-сайти, електронних листів із шкідливими вкладеннями, вірусами, фішингових

електронних листів. Захист даних через шифрування. Малі та середні підприємства повинні гарантувати, що дані, що зберігаються на мобільних пристроях, таких як ноутбуки, смартфони зашифровані. Для даних, що передаються через загальнодоступні мережі, такі як мережі Wi-Fi готелів чи аеропортів, переконайтеся, що дані зашифровані, використовуючи віртуальну приватну мережу (VPN) або доступ до веб-сайтів через безпечне з'єднання за допомогою протоколу SSL/TLS. Переконайтеся, що на їхніх власних веб-сайтах використовується відповідна технологія шифрування для захисту даних клієнтів під час їх передачі через Інтернет.

7. Безпека мережі. Спрощуючи роботу персоналу віддалено, багато МСП дозволяють персоналу використовувати власні ноутбуки, планшети та/або смартфони. Це викликає кілька проблем із безпекою конфіденційних бізнес-даних, що зберігаються на цих пристроях. Одним із способів управління цим ризиком є керування мобільними пристроями. Це дозволить: здійснювати контроль над пристроями, яким дозволено користуватись послугами й системами МСП; на таким пристроях має бути встановлене актуальне сучасне антивірусне ПЗ; доступ до таких пристроїв – через надійні паролі або PIN-код; дистанційно стерти будь-які дані МСП з пристрою, якщо власник пристрою повідомить про втрату чи викрадення пристрою, або якщо робота власника пристрою закінчиться з МСП. Наступна рекомендація – використовувати брандмауери та регулярно перевіряти роботу та налаштування пристроїв, що залучені у віддаленому доступі до ресурсів МСП.

8. Удосконалення фізичної безпеки. Усюди, де міститься важлива інформація, слід застосовувати відповідні засоби фізичного контролю. Наприклад, службовий ноутбук або смартфон не можна залишати без нагляду на задньому сидінні автомобіля. Кожен раз, коли користувач відходить від свого комп'ютера, він повинен заблокувати його. В іншому випадку потрібно увімкнути функцію автоматичного блокування на будь-якому пристрої, який використовується для комерційних цілей. Конфіденційні друковані документи також не слід залишати без нагляду, а якщо вони не використовуються, надійно зберігати.

9. Захист резервних копій. Резервне копіювання має бути регулярним та автоматизованим, бажано шифрувати резервні копії. Проводити тестування щодо здатності відновлення. В ідеалі слід проводити регулярне тестування повного відновлення від початку до кінця.

10. Синхронізувати з хмарними технологіями. Пропонуючи багато переваг, хмарні рішення все ж представляють деякі унікальні ризики, які МСП слід враховувати перед тим, як співпрацювати з постачальником хмарних технологій. ENISA опублікувала «Посібник з хмарної безпеки для малих і середніх підприємств» (ENISA, 2021), до якого малим і середнім підприємствам слід звернутися під час переходу на хмару.

Вибираючи хмарного постачальника, МСП має переконатися, що він не порушує жодних законів чи правил, зберігаючи дані, особливо персональні, за межами ЄС/ЄЕЗ. Наприклад, Загальний регламент захисту даних (GDPR) ЄС вимагає, щоб персональні дані жителів ЄС/ЄЕЗ не зберігалися та не передавалися за межі ЄС/ЄЕЗ, за винятком дуже особливих умов.

11. Захист онлайн-сайтів Вкрай важливо, щоб МСП гарантували, що їхні онлайн-сайти налаштовані та обслуговуються безпечним способом

і що будь-які персональні дані або фінансові деталі, такі як дані кредитної картки, належним чином захищені. Це передбачає проведення регулярних тестів безпеки веб-сайтів для виявлення будь-яких потенційних слабких місць у безпеці та проведення регулярних перевірок для забезпечення належного обслуговування та оновлення сайту.

12. Шукати та ділитись інформацією. Ефективним інструментом боротьби з кіберзлочинністю є обмін інформацією. Обмін інформацією щодо кіберзлочинності є ключовим для того, щоб МСП краще розуміли ризики, з якими вони стикаються. Компанії, які дізнаються про виклики кібербезпеки та про те, як ці проблеми вдалося подолати, з більшою ймовірністю вживуть заходів для захисту своїх систем, ніж якби вони почули подібні подробиці з галузевих звітів або опитувань щодо кібербезпеки.

Захист фінансових систем необхідний для того, щоб запобігти негативним наслідкам для економіки та громадян. Це дозволяє банкам, інвесторам та підприємствам діяти з певною довірою і впевненістю, що їх фінансові активи захищені. Якісний та високий рівень кібербезпеки допомагає захистити фінансову інформацію організації від несанкціонованого доступу, маніпуляцій або крадіжки, допомагає переконатися, що всі фінансові операції є законними та відповідають чинним законам і нормам. Крім того, фінансова кібербезпека допомагає захистити клієнтів і зацікавлених сторін від потенційних фінансових втрат та протидіяти кібератакам, кібершахрайствам.

Список літератури

1. Kuzmenko O.V., Kubalek J., Bozhenko V.V., KushneryovS., Vida I. (2021) An Approach to Managing Innovation to Protect Financial Sector against Cybercrime. Polish Journal of Management Studies. Vol. 24 (2). P. 276-291. https://doi.org/10.17512/pjms.2021.24.2.17

2. Cybersecurity guide for SMEs - 12 steps to securing your business. URL: https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

3. ENISA (2021). Cloud Security Guide for SMEs. Retrieved from: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes