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 В МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВАХ: РОЗРОБКА ТА ВПРОВАДЖЕННЯ СТРАТЕГІЙ ЗАХИСТУ

CYBERSECURITY IN SMALL AND MEDIUM-SIZED ENTERPRISES: DEVELOPMENT AND IMPLEMENTATION OF PROTECTION STRATEGIES

Анастасія Савенко, студентка
Сумський державний університет, Україна
Валерій Яценко, к.т.н, доцент
Сумський державний університет, Україна

В сучасному світі, де все більше підприємств залежать від комп'ютерних систем та електронних пристроїв, кібербезпека стає все більш актуальною та важливою проблемою для малих та середніх підприємств (МСП). У зв'язку з зростаючими загрозами кібербезпеки, захист даних та комп'ютерних систем МСП є великою та складною задачею. Однак, не забезпечення адекватного рівня кібербезпеки може призвести до надмірних витрат на відновлення даних та втрати довіри споживачів. Приділення уваги проблемі кібербезпеки в МСП є ключовим для забезпечення їх сталого розвитку та позиції на ринку.

Метою даної роботи є дослідження питання кібербезпеки в малих та середніх підприємствах, а також розробки та впровадження стратегій захисту.

В сучасному світі інноваційних технологій людська діяльність переходить до кіберпростору, що полегшує та покращує її. Таким чином, держава, приватні підприємства, соціально-адміністративний сектор тримають за ціль повну цифровізацію систем та баз даних. При цьому проблема забезпечення безпеки у кіберпросторі залишається не до кінця пропрацьовоною та потребує значних ресурсів з боку держави, однак через недофінансування та неможливість охопити безпеку кожної фізичної та юридичної особи окремо, безперебійне функціонування інформаційних та комунікаційних систем знаходиться під загрозою. На базі такого переміщення, виник та розпочав свій розвиток приватний сектор із забезпечення надійності безпеки у кіберпросторі, висвітлення основних функцій та необхідності якого є актуальним як для підприємців, що хочуть скористатися послугами IT компаній, так і робочих кадрів та підприємців у сфері кібербезпеки, що тільки розпочинають чи планують розпочати свою діяльність.

З прогресом технологій та підвищенням рівня підключення до мережі Інтернет, МСП стають все більш вразливими до кібератак та кіберзлочинності. У малих та середніх підприємств часто недостатньо ресурсів та експертизи в

області кібербезпеки, що створюєся зону вразливості для хакерів та кіберзлочинців. До загроз для МСП можна віднести наступні:

– фішингові атаки та віруси, оскільки часто призводять до викривлення або втрати важливої інформації;

– кібератаки, які можуть призвести до відключення важливих систем та збоїв у роботі підприємства;

– несанкціонований доступ до конфіденційної інформації та даних клієнтів;

– втрати даних та відмови забезпечення правильного функціонування систем.

Забезпечення кібербезпеки є надзвичайно важливим для малих та середніх підприємств (МСП) з наступних причин:

1. Обмежені ресурси: МСП, зазвичай, мають обмежені фінансові, технічні та людські ресурси для вирішення кібербезпекових проблем. Вони можуть не мати великого бюджету на кібербезпеку або доступу до широкого кола експертів. Це робить їх вразливими перед кіберзлочинцями, які можуть спрямувати свої атаки на слабкі місця;

2. Цінність даних: МСП зберігають і обробляють значну кількість цінних даних, таких як фінансова інформація клієнтів, інтелектуальна власність, персональні дані тощо. Компрометація цих даних може призвести до серйозних фінансових втрат, порушення довіри клієнтів та збитків у репутації підприємства;

3. Законодавчі вимоги: Багато країн встановлюють обов'язкові законодавчі вимоги щодо кібербезпеки, особливо щодо захисту персональних даних. Невиконання цих вимог може призвести до значних адміністративних санкцій та штрафів для МСП;

4. Постійні загрози: Кіберзлочинці постійно розвиваються та удосконалюють свої методи атак. Малі та середні підприємства, які не приділяють належної уваги кібербезпеці, можуть стати привабливою мішенню для кіберзлочинців.

Якщо розглядати попит на українському ринку, то можна навести дані з проведеного опитування з кібербезпеки бізнесу в Україні. Опитування проводили протягом майже двох місяців узимку, у ньому взяли участь 150 українських підприємств. Найбільше було компаній зі сфер ритейлу (23%), IT (14%), державного сектора (14%). Також в опитуванні взяли участь середній бізнес, фінансові, страхові компанії та інші. 91% організацій вважають, що мають повний або достатньо повний набір технологій. 52% зазначили, що можуть бачити стан речей в IT-інфраструктурі. Рівень повноцінного використання таких технологій, як багатофакторна автентифікація (MFA), захисний DNS, контроль взаємодії пристроїв у мережі (NDR), управління подіями кібербезпеки (SIEM), та іншого зрідка перевищує 40%. Від 50% до

60% респондентів розповіли, що взагалі не використовують такі технології, як програмування систем безпеки, кіберрозвідка, захист із використанням методів обману тощо. Також лише 41% компаній зазначили, що мають виокремленого CISO (керівник відділу IT-безпеки, директор з IT-безпеки).

Оскільки кібербезпека є критично важливим елементом успішної діяльності МСП, розробка та впровадження ефективних стратегій та заходів захисту є необхідними. Ці заходи можуть включати наступні елементи:

– створення стратегії та політики кібербезпеки, яка включає плани на випадок кібератак та інші ризики;

– встановлення міцних паролів та керування доступом до важливої інформації та систем;

– застосування системи бекапу даних та створення копій безпеки;

– забезпечення оновлення програмного забезпечення та антивірусних програм для дотримання стандартів безпеки;

– запровадження мережевої безпеки та систем поширення даних.

Забезпечення високого рівня кібербезпеки в МСП є критично важливим для успішної діяльності та майбутнього розвитку. Розробка та впровадження ефективних стратегій та заходів захисту надасть підприємству можливість протидіяти загрозам і захистити комп'ютерні системи та інформацію, збережений у них. Навчання працівників та відповідність вимогам щодо кібербезпеки повинні бути складовими частинами успішної політики цього питання. МСП повинні зробити все можливе, щоб захистити свою інформацію та зберегти довіру клієнтів та інвесторів.

У сучасному світі, де цифрові технології займають все більш важливу роль в бізнес-середовищі, кібербезпека стає вирішальною складовою для успіху малих та середніх підприємств (МСП). Малим та середнім підприємствам дедалі більше загрожують кібератаки, оскільки вони можуть бути менш захищеними та мати обмежені ресурси для кібербезпекових заходів.

Список літератури

1. Лише 41% компаній мають директора з IT-безпеки, третина не перевіряє аварійне відновлення – дослідження з кібербезпеки - ITC.ua. ITC.ua. URL: https://itc.ua/ua/articles/lyshe-41-kompanij-mayut-dyrektora-z-it-bezpeky-tretyna-ne-pereviryaye-avarijne-vidnovlennya-doslidzhennya-z-kiberbezpeky/ (дата звернення: 28.03.2023).

2. Microsoft Digital Defense Report 2022. Microsoft. URL: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022 (date of access: 28.03.2023).

3. Про основні засади забезпечення кібербезпеки України : закон від 05.10.2017 р. № № 2163-VIII. URL: https://zakon.rada.gov.ua/ laws/show/2163-19#Tet

4. Захист персональних даних за правилами GDPR – ECPL.com.ua. URL: https://ecpl.com.ua/news/zakhyst-personal-nykh-danykh-za-pravylamy-gdpr/

5. Трофіменко О. Г., Трофименко Е. Г. Кібербезпека України: аналіз сучасного стану. URL: http://dspace.onua.edu.ua/bitstream/ handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence (дата звернення: 28.03.2023).