**Тема 12. Оцінка ризиків та політика інформаційної безпеки.**

**Оцінка ризиків для компанії «CloudTech Solutions»**

*Виконано за методологією OCTAVE з урахуванням стандартів ISO/IEC 27001, NIST SP 800-30, GDPR, ЗУ «Про захист персональних даних»*

1. **Ідентифікація активів**

|  |  |  |
| --- | --- | --- |
| **Актив** | **Критичність** | **Обґрунтування** |
| Хмарні сервери | Висока | Основна платформа для клієнтських сервісів. Втрата доступу загрожує зупинці бізнесу |
| Мережева інфраструктура | Висока | Забезпечує зв’язок, VPN, захист. Компрометація чи проникнення в системи |
| Системи зберігання даних | Висока | Містять критичні дані клієнтів. Втрата даних це порушення GDPR, фінансові втрати |
| Клієнтські застосунки | Середня | Інтерфейс доступу, важливий для UX, але не містить критичних даних |
| Офісна ІТ-система | Середня | Підтримка внутрішніх процесів. Зупинка, віддати в ремонт, поломка загрожує зниженню ефективності, але не зупинці бізнеса |
| *ISO/IEC 27001 Annex A.8.1.1 - Ідентифікація активів*  *NIST SP 800-30 - Identify assets and asset owners* | | |

1. **Ідентифікація загроз і вразливостей**

|  |  |  |
| --- | --- | --- |
| **Загроза/Вразливість** | **Вірогідність** | **Обґрунтування** |
| DDoS - атаки | Середня | 2 випадки на рік, зростання за останні 3 роки |
| Витоки даних через слабкий DLP | Висока | 5 випадків на рік, стабільна повторюваність |
| Інфікування шкідливим ПЗ | Висока | 15 випадків на рік, зниження, але все ще значна кількість |
| Вразливості хмарних серверів | Середня | 20% серверів мають критичні вразливості |
| Фішинг/соціальна інженерія | Висока | Відсутність навчання, слабкий захист пошти |
| *NIST SP 800-30 - Identify threats and vulnerabilities*  *ISO/IEC 27005 - Risk assessment process*  *GDPR - Security of processing* | | |

1. **Оцінка ризиків за OCTAVE**

*Частота та повторюваність*

|  |  |  |
| --- | --- | --- |
| **Загроза** | **Частота** | **Повторюваність** |
| DDoS | 2 на рік | Зростає |
| Витоки даних | 5 на рік | Стабільна |
| Шкідливе ПЗ | 15 в рік | Знижується |
| Вразливості хмарних серверів | 20% | Середня |
| Фішинг | Не фіксується але висока ймовірність | Постійна |
| *OCTAVE - Identify infrastructure vulnerabilities*  *NIST SP 800-30 - Determine likelihood and impact* | | |

1. **Стратегії мінімізації**

*DDoS*

* Впровадження CDN та WAF
* Контракт з DDoS-захистом (Cloudflare, Arbor)
* Моніторинг трафіку через SIEM
* Резервні канали
* Тестування навантаження
* План реагування на DDoS

*\*ISO/IEC 27001 Annex A.13.1.1 - Network controls*

*Витоки даних*

* Впровадження повноцінної DLP
* Шифрування даних (AES-256)
* Аудит доступу
* Навчання персоналу
* NDA/DPA з підрядниками
* Контроль шерінгу в G-Drive

*\*GDPR Art. 32, 33*

*\*ISO/IEC 27001 Annex A.18.1.4 - Privacy and protection of PII*

*Шкідливе ПЗ*

* Встановлення EDR на всі сервери
* Оновлення антивірусного ПЗ
* Сканування систем
* Обмеження прав встановлення ПЗ
* Навчання персоналу щодо фішингу
* Sandbox для підозрілих файлів (*!наголосити на провести навчання!*)

*\*ISO/IEC 27001 Annex A.12.2.1 - Controls against malware*

*Вразливість хмарних серверів*

* Аудит конфігурацій (ScoutSuite, Prowler)
* MFA для доступу
* IAM політики
* Логування через CloudTrail
* Шифрування даних
* Контроль оновлень

\*ISO/IEC 27017 - Cloud security controls

\**NIST SP 800-53 Rev. 5 - AC, SC, SI families*

*Фішинг та соціальна інженерія*

* Навчання персоналу
* Фільтрація пошти
* DMARC/SPF/DKIM
* Симуляція атак
* Механізм повідомлення про фішинг
* Обмеження доступу через email

*\*ISO/IEC 27001 Annex A.7.2.2 - Information security awareness*

*\*NIST SP 800-50 - Building an awareness program*

1. **Розробка планів з обробки ризиків**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ризик** | **Підхід** | **Обґрунтування** | **Заходи** |
| DDoS | Зменшення | Можна знизити вплив через технічні засоби | CDN, WAF, резервні канали |
| Витоки даних | Зменшення | Повністю уникнути неможливо, але можна контролювати | DLP, шифрування, аудит |
| Шкідливе ПЗ | Зменшення | Вплив можна знизити через EDR та навчання | EDR, sandbox, оновлення |
| Вразливості хмарних серверів | Зменшення | Виявлені вразливості можна усунути | Аудит, MFA, IAM |
| Фішинг | Зменшення | Людський фактор - ключовий, але піддається навчанню | Тренінги, фільтри, DMARC |
| *ISO/IEC 27005 - Risk treatment*  *NIST SP 800-30 - Risk response strategies* | | | |