УДК 004.056.5 https://doi.org/10.30837/IYF.PCEIP.2024.159

СТРАТЕГІЇ АДАПТАЦІЇ CIS CONTROLS ДО СПЕЦИФІКИ СЕКТОРУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Уманець М.С.
Науковий керівник – Євгеньєв А.М.
Харківський національний університет радіоелектроніки
61166, Харків,просп.Науки,14, каф. БІТ
e-mail:mariia.umanets@nure.ua

This paper presents the main steps to start implementing CIS CONTROLS for any system or organization, both private and public sector. The key stages are considered, the observance of which will contribute to the increase of the level of cybersecurity of information systems, reduction of the risks of cyberattacks and their consequences, and effective use of CIS Controls to protect information systems.

Сучасні стандарти та законодавство вимагають від організацій впровадження специфічних заходів безпеки та більш точного та адаптованого контролю. Керування CIS Controls - це пріоритетний набір дій, розроблений світовою IT-спільнотою з метою підвищення рівня безпеки інформаційних систем та даних [1]. CIS Controls визначають ключові кроки, які організації повинні вживати для захисту від загроз, включаючи кібератаки, витоки даних та зловживання привілеями. Адаптація цих контролів до конкретних потреб сектору інформаційної безпеки дозволяє забезпечити ефективний захист, враховуючи специфіку діяльності та ризики даного сектору.

Для ефективного впровадження та адаптації CIS Controls до певної інформаційної системи необхідно дотримуватися певної стратегії, яку поділено на кроки [2].

Першим рекомендованим кроком є «Проведення інвентаризації активів». Важливо з самого початку розуміти, що саме підлягає захисту, цей крок відповідає Критичним контролям безпеки 1 і 2:

- CSC 1. Інвентаризація та контроль апаратних засобів. (Активне керування всіма апаратними пристроями в мережі так, щоб доступ до них мали лише авторизовані пристрої.)
- CSC 2: Інвентаризація та контроль програмних активів. (Активне керування усім програмним забезпеченням у мережі, щоб лише дозволене програмне забезпечення було встановлене та могло виконуватися.)

На другому етапі необхідно провести «Вимірювання засобів контролю активів», який включає безперервне управління вразливостями, контрольоване використання адміністративних привілеїв, безпечну конфігурацію апаратного та програмного забезпечення на мобільних пристроях, ноутбуках, робочих станціях та серверах, захист електронної пошти та веб-браузерів, захист від

шкідливого програмного забезпечення, можливість відновлення та захист даних.

Третій крок – це захист зовнішнього контуру мережі. На цьому кроці необхідно забезпечити обмеження та контроль мережевих портів, протоколів і служб. Створити та активно керувати конфігурацією безпеки пристроїв мережевої інфраструктури, використовуючи суворий процес управління конфігурацією та контролю змін, щоб запобігти використанню зловмисниками вразливих сервісів та налаштувань, а також забезпечити контроль бездротового доступу.

Крок чотири. Виявлення та реагування на інциденти [3]. Невід'ємною частиною впровадження контролю є розробка інфраструктури моніторингу, аналізу та реагування на інциденти для швидкого виявлення атаки, а потім ефективного обмеження збитків, усунення присутності зловмисника та відновлення цілісності мережі та систем.

П’ятий крок це навчання та контроль користувачів, так як люди є найслабшою ланкою в ланцюгу безпеки. Плануючи та впроваджуючи навчання та моніторинг користувачів рекомендовано звернути увагу на такі ключові моменти як: захист електронної пошти та веб-браузерів, контрольоване використання адміністративних привілеїв, впровадження програми підвищення обізнаності та навчання з питань безпеки.

Фінальним, шостим кроком розглянутої стратегії є тестування. Після впровадження засобів контролю доцільно використовувати такі інструменти, як тестування на проникнення, щоб переконатися, проведена робота виконана успішно. Це необхідно робити на регулярній основі, з метою перевірки загальної сили захисту організації імітуючи цілі та дії зловмисника.

CIS Controls - це базові засоби контролю безпеки, які суб’єкти як приватного так і публічного сектору можуть використовувати для вдосконалення своєї програми кібербезпеки. Вони дають чітке уявлення про те, чого не вистачає у запезпечені безпеки, і можуть бути використані як дорожня карта, навіть впровадження перших 4-5 наборів засобів контролю може значно підвищити стійкість компанії. CIS Controls зосереджені не лише на впровадженні, але й на забезпеченні гарантій за допомогою реалізації, вимірювання, автоматизації та звітності.

Список використаних джерел

1. CIS controls v8. Official edition.

2. Marotta L. 8 steps to successfully implement the CIS top 20 controls | rapid7 blog. *Rapid7*. URL: https://www.rapid7.com/blog/post/2020/04/07/8-steps-to-successfully-implement-the-cis-top-20-controls-in-your-organization/ (дата звернення: 01.03.2024).

3. Ушатов В., Сєвєрінов О.В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. – Харків: ХНУРЕ, 2019. - С. 104–105.