КОМПЛЕКСНІ ЗАХОДИ З КІБЕРБЕЗПЕКИ ТА ІНЖЕНЕРІЇ ДЛЯ ЗАХИСТУ КІБЕРФІЗИЧНИХ СИСТЕМ

Скидан В.Л., здоб. ОС «магістр»
Науковий керівник – канд. екон. наук, доц. **І.С. Андрющенко**
Державний біотехнологічний університет

Cyber-physical systems (CPS) є життєво важливими компонентами в різних сферах критичної інфраструктури, включаючи національну електромережу, транспорт, охорону здоров'я та оборону. Ці системи вимагають високого рівня стабільності, продуктивності, ефективності та надійності. Однак, через свою складність та кібер-фізичний зв'язок, вони є вразливими до загроз порушення безпеки, коли люди, процеси чи технології зазнають атак або системи управління ризиками виявляються недосконалими. Зловмисники часто націлені на конфіденційні дані, що робить захист CPS надзвичайно важливим [1]. Оскільки використання CPS продовжує зростати, загрози для цих систем ймовірно, збільшуватимуться. Щоб зменшити втрати та забезпечити відновлення після потенційних атак, організації повинні впроваджувати ефективні заходи кібербезпеки. Для контролю та відновлення після атак та їхніх наслідків дуже важливо мати інформацію від експертів з досліджень та галузевих експертів.

Управління ризиками безпеки, пов'язаними з CPS, є безперервним процесом. Він включає в себе розуміння рейтингів ризиків, впровадження правильних процесів і засобів контролю на основі рівня толерантності організації до ризиків, а також вжиття коригувальних заходів у відповідь на події. Управління ризиками відіграє вирішальну роль у виявленні та проактивному вирішенні потенційних управлінських і технічних проблем [2]. Однак управління ризиками в CPS є складним завданням через складність систем, мінливі рівні ризиків, загрози людського фактору та можливість каскадних збоїв. Загрози в одній частині CPS можуть поширюватися на інші частини через взаємопов'язаність галузей нейронних мереж та комп'ютерної кібербезпеки. З ростом нашої залежності від технологій зростає і потреба в безпечних системах. Комп'ютерні інженери займаються проектуванням та розробкою апаратних та програмних систем, а професіонали з кібербезпеки грають важливу роль у забезпеченні їхньої безпеки. В сучасну цифрову епоху взаємодія між цими двома галузями є дуже важливою.

З урахуванням зростання кількості кіберзагроз, вирішення проблем безпеки стало пріоритним для організацій по всьому світу. Це

передбачає впровадження надійних заходів безпеки, таких як брандмауери, технології шифрування та безпечні практики кодування. Крім того, у сфері кібербезпеки зловмисники використовують різні загальні вектори загроз для використання вразливостей в інформаційно-комунікаційних системах. Розуміння цих векторів має вирішальне значення для розробки ефективних контрзаходів і захисту від потенційних загроз. Деякі з найпоширеніших векторів загроз включають:

- шкідливе програмне забезпечення, в тому числі віруси, хробаки, трояни та програми-вимагачі, які можуть проникати в системи через заражені файли, завантаження або вкладення електронної пошти, ставлячи під загрозу дані та цілісність системи;

- фішингові атаки, які часто пов'язані з оманливими електронними листами або веб-сайтами, виманюють у користувачів конфіденційну інформацію, наприклад, паролі або дані кредитних карток, видаючи себе за довірені особи;

- атаки типу «відмова в обслуговуванні» (DoS) та «розподілена відмова в обслуговуванні» (DDoS), ці атаки перевантажують мережеві ресурси або послуги, роблячи їх недоступними для законних користувачів;

- інсайдерські загрози, особи з авторизованим доступом до систем можуть становити загрозу, навмисно чи ненавмисно порушуючи безпеку, здійснюючи витік конфіденційної інформації або беручи участь у зловмисних діях;

- вразливості нульового дня, зловмисники націлені на невиявлені вразливості програмного забезпечення, експлуатуючи їх до того, як розробники встигнуть випустити виправлення або оновлення.

Щоб проілюструвати реальні наслідки цих поширених векторів загроз, розглянемо декілька прикладів:

- WannaCry поширилася по всьому світу, використовуючи відому вразливість у системах Windows. Він шифрував файли користувачів і вимагав викуп за розшифрування. Від цієї атаки постраждали лікарні, підприємства та державні установи, що підкреслило важливість негайного застосування патчів безпеки [3].

- Витік даних LinkedIn 2012 році LinkedIn зазнав значного витоку даних, в результаті якого були розкриті облікові дані понад 100 мільйонів користувачів. Порушення стало результатом поєднання слабкого зберігання паролів і неналежних заходів безпеки, що підкреслює необхідність надійного управління паролями та шифрування.

- Порушення даних цільової роздрібної торгівлі 2013 році кіберзлочинці викрали інформацію про кредитні картки з систем торгових точок Target. Порушення сталося через скомпрометовані облікові дані постачальника HVAC, що демонструє ризики, пов'язані з уразливістю ланцюгів постачання. Ці реальні приклади демонструють відчутний вплив поширених векторів загроз і підкреслюють необхідність проактивних заходів кібербезпеки, включаючи регулярні оновлення, навчання співробітників і надійний контроль доступу [3].

Тож, можна зробити висновок, що критичні об'єкти інфраструктури стають все більш вразливими до кібератак, які можуть порушити бізнес-операції та вплинути на зацікавлені сторони. Інтегрована система управління ризиками кібербезпеки для об'єктів критичної інфраструктури може систематично аналізувати ризики та пропонувати плани контролю над ними, забезпечуючи безперервність бізнесу. Кожна критична інфраструктура повинна впровадити ефективний процес управління ризиками, щоб захистити зацікавлені сторони від фінансових, організаційних та репутаційних втрат.

Інформаційні джерела

1. Türkmen, E.; Soyer, A. The Effects of Digital Transformation on Organizations. In Handbook of Research on Strategic Fit and Designin Business Ecosystems: Advances in E-Business Research; IGI Global: Hershey, PA, USA, 2020; pp. 259–288.

2. Hess, T.; Matt, C.; Benlian, A.; Wiesböck, F. Options for Formulating a Digital Transformation Strategy. MIS Q. Exec. 2016, 15,123–139.

3. Preventing WannaCry Ransomware (WCRY) attack using Trend Micro Products. URL:https://success.trendmicro.com/dcx/s/solution/ 1117391-preventing-wannacry-wcry-ransomware-attacks-using-trend-micro-products?language=en_US&sfdcIFrameOrigin=null