УДК 004.056
DOI: 10.31673/2409-7292.2021.013034

Заікін С.С., Кітура О.В.

МОДЕЛЬ ПЕРЕДБАЧЕННЯ ІНСАЙДЕРСЬКОЇ ЗАГРОЗИ В ОРГАНІЗАЦІЇ

У статті розглянуто поняття «інсайдерська загроза» та «інсайдер». Визначено загальні методи використання кіберзлочинцями інсайдерських загроз для компрометації мережевого середовища організації для отримання доступу до цінних активів. Досліджено різновиди інсайдерських загроз та їх критичність для організацій щодо боротьби з цими загрозами для зменшення ризику. Зроблено висновок, що жоден підхід не може вирішити проблему безпеки. З метою пом'якшення інсайдерської загрози необхідні додаткові дослідження в галузі інсайдерських загроз кібербезпеки, і слід визначити правильний підхід до боротьби зі зловмисною інсайдерською загрозою з різних точок зору. Зазначено, що організації можуть запровадити деякі основні заходи, які можуть зменшити кількість випадків інсайдерських загроз до мінімуму.

Ключові слова: інсайдер, інсайдерська загроза, модель передбачення, кіберзахист

Вступ.

Інформаційна безпека, як відомо, має справу з двома категоріями загроз: зовнішніми і внутрішніми. Саме до останнього типу відносяться інсайдерські загрози. Діяльність інсайдерів, в більшості випадків, має ненавмисний характер, саме тому її важко передбачити і знешкодити. Для цього необхідно задіяти весь арсенал доступних засобів ІБ. Найбільш поширені канали витоку відносяться до категорії ненавмисного розкриття, через необізнаність або недисциплінованості співробітників. Це і банальна «балаканина співробітників», і відсутність уявлень про правила роботи з конфіденційними документами, і невміння визначити які документи є конфіденційними. Навмисний «злив інформації» зустрічається значно рідше, зате в даному випадку інформація «зливається» цілеспрямовано і з найбільш небезпечними наслідками для організації [1].

Стан проблеми протидії інсайдерським загрозам у світі.

Загрози, які інсайдери створюють для державних організацій, підприємств та установ, продовжують викликати занепокоєння. Сучасні дослідження дають однозначні докази, які підкреслюють тяжкість та поширеність цієї загрози на сьогоднішньому бізнесі. Згідно з глобальним звітом за 2020 рік, середня глобальна вартість інсайдерських загроз за останні два роки зросла на 31% - до 11,45 млн.доларів, а кількість інцидентів у цей період зросла на 47%. Завдяки оцінці та аналізу інцидентів проблему внутрішньої загрози можна краще зрозуміти та вирішити.

Наприклад, звіт Агентства Європейського Союзу з кібербезпеки (ENISA) за 2020 рік [2] класифікував чотири основних інциденти/дії, пов'язані з інсайдерами, наступним чином: зловживання привілеями (60%), неправильне використання даних (13%), використання не схвалене обладнання (10%) та зловживання привілеями (10%). Відповідно до звіту ENISA, 27% випадків порушення даних були спричинені людським фактором або недбалістю, і, згідно з дослідженням, фішинг (67%) є основною проблемою у випадку ненавмисних погроз інсайдером. Слабкі або повторно використані паролі (56%), розблоковані пристрої (44%), практика спільного використання паролів (44%) та незахищені мережі Wi-Fi (32%) також були частиною списку ненавмисних інсайдерських загроз. Більше того, у звіті зазначено, що поширеність цих атак зросла до 56%, тоді як 30% організацій вважають, що вони зазнали занадто багато атак. Отже, це породжує вирішальну необхідність попередніх оборонних дій, які повинні здійснюватись організаціями для боротьби з цією загрозою.

Як правило, бізнес інвестує в засоби захисту, щоб зміцнити свою мережу від зовнішніх шкідливих атак. Однак їм не вдається застосувати захист від потенційних загроз зловмисних або скомпрометованих інсайдерів. Інсайдери можуть зловживати своїм дозволеним доступом до критично важливих систем і врешті-решт викрасти або модифікувати системи даних з метою зловмисних намірів чи фінансової вигоди. Інсайдерська загроза націлена не лише на підприємства приватного сектору, а й на державні установи та критичну інфраструктуру з

мотивів, починаючи від грошових прибутків та промислового шпигунства, закінчуючи перевагами бізнесу та саботажем [3].

Оскільки інсайдери мають доступ до цінних інформаційних ресурсів, недоступних для сторонніх осіб, збитки, спричинені атаками інсайдерів, можуть бути руйнівними. Крім того, ці загрози зростають за масштабами, масштабами та витонченістю; таким чином, наголошуючи на критичній необхідності організацій застосовувати сучасні методи безпеки.

За даними Центру захисту національної інфраструктури (CPNI), інсайдер - це той, хто експлуатує або має намір використовувати їх законний доступ до активів організації з несанкціонованими цілями. Крім того, довіреним особам надаються облікові дані, такі як ім'я користувача та паролі, отже, пропонуючи шлюз до інформаційної мережі організації, тобто приховування в інфраструктурі не вимагає зусиль. Ця загроза є досить складною, щоб порушити принципи безпеки конфіденційності, цілісності та доступності, які повинні бути гарантовані для будь-якої захищеної оборонної системи. Відповідно до недавнього опитування, 27% від загальної кількості випадків кіберзлочинів передбачалося здійснити інсайдерами, а 30% респондентів зазначили, що руйнування, спричинені інсайдерами, були більш серйозними, ніж збитки, завдані зовнішніми зловмисниками.

Звіт ENISA продемонстрував небезпеку внутрішньої загрози для безпеки організацій, втілюючи критичну потребу в їх вирішенні. Ця робота спрямована на розширення знань про те, як інсайдерська загроза розширюється, та на деталізацію комплексних дій, необхідних організаціям для вирішення критичних ризиків, які вона створює. Це обов'язково, оскільки організації постійно спрямовують фінансування на традиційні стратегії, які не в змозі захистити від внутрішньої загрози. Представлено, як технології/інструменти, що використовуються інсайдерами, можуть розширюватися на всіх семи етапах ланцюга вбивств, які розпізнаються в багатьох кібератаках. Серед інструментів, які використовують інсайдери, у цій роботі пропонується пошаровий оборонний підхід, що включає політику, організаційну культуру та технічне середовище для боротьби із загрозою.

Багато заходів, спрямованих на виявлення інсайдерських загроз, розвиваються під впливом підходів, які використовуються для виявлення зовнішніх загроз. Широко використовуються підходи, розроблені для виявлення вторгнень, в тому числі моніторинг мережі організації [3]. Проте, ці підходи не завжди ефективні для виявлення внутрішніх загроз і можуть давати велику кількість хибно позитивних результатів. Таким чином, ці підходи мають обмежене застосування при виявленні інсайдерських загроз. В тому числі, системи виявлення вторгнень використовують сигнатури атак і не можуть виявити дії, які не залишають записи в журналах системи.

Також заходи з протидії внутрішнім загрозам необхідно класифікувати на основі етапу їх дії:

Запобігання. Заходи, спрямовані на запобігання виникненню внутрішньої загрози, в тому числі заходи по прогнозуванню інсайдерських атак на основі потенційних показників. Внутрішня політика є основою для дотримання нормативних вимог і запобігання інсайдерських інцидентів. Політика визначає і регулює дії і поведінку персоналу в організації. Однак сама по собі політика не дуже корисна, якщо вона не підкріплена наслідками. Ці наслідки мають найбільший вплив на внутрішню загрозу.

Виявлення. Заходи, спрямовані на виявлення наявності внутрішньої загрози, якщо атака відбувається або вже відбулася. Існує кілька методів виявлення атак ззовні, проте, виявляти інсайдерські дії набагато складніше. Інсайдерські дії можуть виявлятися за допомогою інструментів моніторингу та ведення журналів, а також інформаторів і приманок.

Реагування. Заходи, що застосовуються для усунення внутрішньої загрози після її виникнення. Ці заходи можуть бути коригуючими і присікати, щоб звести до мінімуму наслідки. Організації можуть також вживати відповідних заходів щодо відповідних інсайдерів.

На перший погляд, реакція на внутрішню загрозу здається досить простою: розслідування та судовий процес. Однак в дійсності реакція на внутрішні загрози може бути

досить складною. Організації, як правило, приховують загрозу від громадськості через острах негативних відгуків у пресі. У тих випадках, коли реакцією були судові позови, організації не відшкодовували збитки, а карали відповідних інсайдерів. Для громадськості це може виглядати так, ніби організація робить все, що в її силах, щоб захистити себе. На основі вищезазначеного можна зробити висновок, що незважаючи на зростаючу потребу в методі, здатному допомагати виявляти інсайдерські загрози, на даний момент відсутній універсальний підхід, здатний комплексно вирішувати проблему виявлення внутрішніх загроз і протидії їм, тому що виявлення інсайдерської загрози можливо тільки при наявності адекватної моделі, яка описує організацію, її інформаційні активи і працівників.

Метою даної статті є розроблення моделі передбачення інсайдерських загроз в організації на основі поєднання технічних та психологічних аспектів безпеки.

Модель передбачення інсайдерських загроз

Запропонована модель передбачення інсайдерських загроз зосереджена на поєднанні двох підходів – реалізації технічного методу та психології. Перша частина моделі – це аналіз нетипової поведінки в інформаційних системах в режимі реального часу на основі інформації, зібраної за допомогою Honeypot, системи виявлення вторгнень та системних сигналів.

Друга частина моделі – це аналіз такого компоненту як психологічне профілювання (визначення рівня стресу працівників та ін). На рис. 1 представлена модель передбачення інсайдерських загроз [4].

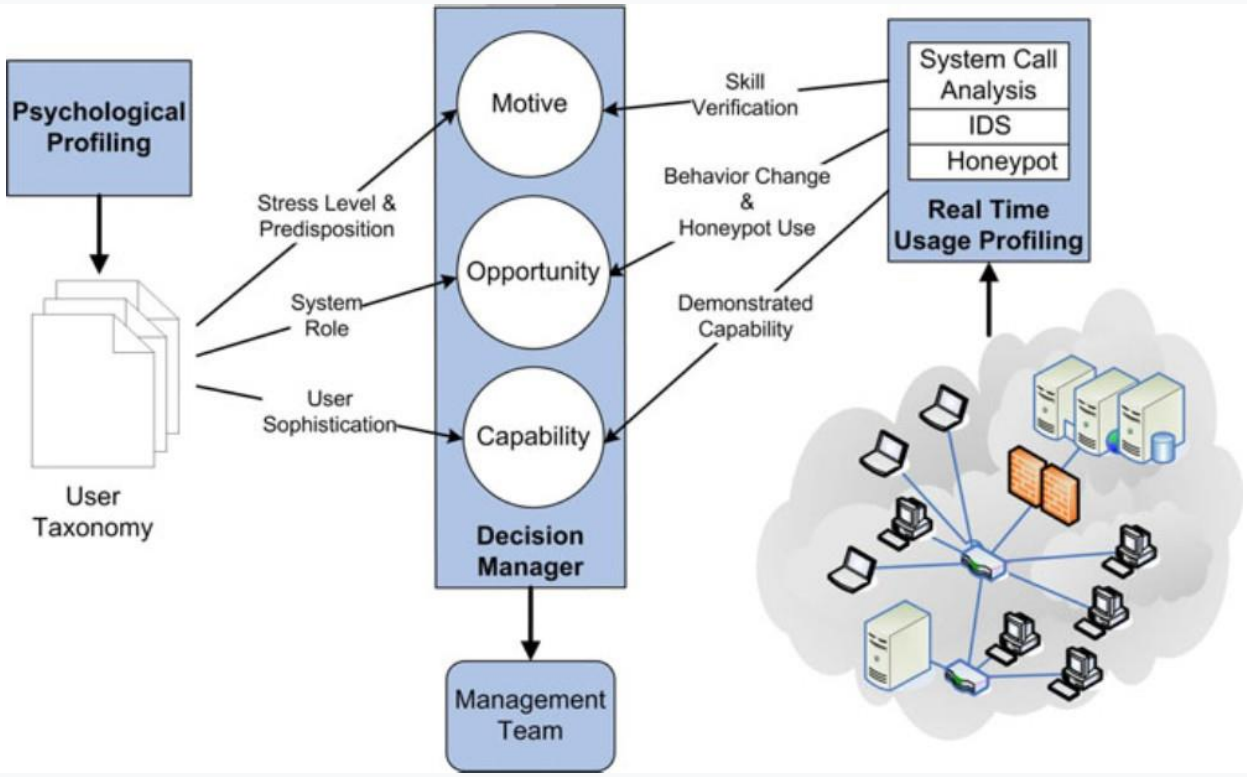

Рис. 1. Модель передбачення інсайдерських загроз

Щоб дозволити управлінській команді передбачити потенційну загрозу інсайдерів, вони виявили взаємозв'язок між усіма параметрами, зібраними з джерел психологічної профілактики та технічного контролю, з трьома факторами: мотивацією, можливостями та здатностями, де кожен фактор отримує оціночний бал у такій формі: низький (1-2), середній (3-4) та високий (5-6).

Психологія – це наукове вивчення людського розуму та його функцій, особливо тих, що впливають на поведінку в певному контексті. Honeypot – це пастка, встановлена для виявлення, відхилення або якимось чином протидії спробам несанкціонованого використання інформаційних систем. Система виявлення вторгнень (IDS) (IDS) – це пристрій або програмний додаток, який контролює мережеві або системні дії на предмет зловмисних дій. System Calls – це те, як програма запитує послугу у ядра операційної системи, яка зазвичай не має дозволу на запуск.

Мотив користувача M_i оцінюється за трьома параметрами: схильність до зловмисної поведінки P_i, рівень стресу S_i та перевірка вміння V_i.

$$M_i = f(P_i + S_i + V_i). \quad (1)$$

Для вимірювання рівня схильності до зловмисної поведінки вони використовували Індекс комп'ютерної злочинності (CCISLQ) [5]. Другим параметром для вимірювання є рівень стресу, який базується на психометричному тесті [6], що оцінює як особистий, так і професійний стрес. Нарешті, рівень перевірки навичок задекларував навички користувачів під час психометричного тесту.

Можливість для користувача O_i оцінюється за трьома параметрами: зміна робочої поведінки Bi, системна роль Ri та використання медової точки H_i.

$$O_i = f(B_i + R_i + H_i). \quad (2)$$

Зміна робочої поведінки, виміряна під час взаємодії з IT-інфраструктурою, може свідчити про те, що користувач знаходиться в процесі пошуку можливої цілі (вразливості) в системі. Другим параметром, який потрібно виміряти, є роль користувацьких систем, яка базується на позиції організаційної структури користувача, яка може бути «початківцем», «просунутим» або «адміністратором». Нарешті, якщо користувач взаємодіє із системою Honeypot, це буде свідчити про високий ризик загрози.

Здатність користувача C_i оцінюється за двома параметрами: продемонстрована спроможність D_i та вишуканість користувача S_i.

$$C_i = f(D_i + S_i). \quad (3)$$

Продемонстрована здатність вимірюється за допомогою засобів аналізу системних викликів та IDS, де досвідченість користувача вимірюється за допомогою психометричного тесту.

Оцінка загрози T_i вимірюється за допомогою системи підрахунку балів (таблиця 1), суми мотивів та можливостей. T_i ділить користувача на чотири категорії: відсутність ризику (3, 4), середній ризик (5, 6), високий ризик (7, 8) та дуже високий ризик (9) [6].

$$T_i = f(M_i + O_i + C_i). \quad (4)$$

Перевагою запропонованої моделі є її простота та зручність у використанні. Оцінки базуються на думці експертів, що дає можливість уникнути певного формалізму у порівнянні з машинним оцінюванням.

Разом з тим у такому підході є і обмеження. Перше обмеження стосується IDS, оскільки це залежить від моніторингу портів мережевих комутаторів, який не може аналізувати зашифровані дані або трафік через зашифровані канали як захищена віртуальна приватна мережа (VPN) або захищене веб-з'єднання за допомогою рівня захищених сокетів (SSL).

Таблиця 1

Розрахунок показників інсайдерських загроз

Мотивація	Можливість	Здатність		
		Низький	Середній	Високий
Низький	Низький	3	4	5
	Середній	4	5	6
	Високий	5	6	7
Середній	Низький	4	5	6
	Середній	5	6	7
	Високий	6	7	8
Високий	Низький	5	6	7
	Середній	6	7	8
	Високий	7	8	9

Друге обмеження полягає у використанні системних журналів, оскільки будь-які дії, вжиті в системі, повинні реєструватися та оброблятися в режимі реального часу, який буде обмежений ресурсами та характеристиками інформаційної інфраструктури.

Для підприємств надзвичайно важливо визначити технології, інструменти та практики, які кіберзлочинці використовують для здійснення інсайдерських атак внутрішньої загрози. Це пов'язано з потенційним руйнуванням, яке вони спричиняють – приклади включають зупинення виконання тих чи інших операцій, втрату інтелектуальної власності та шкоду репутації, оскільки вони мають легкий доступ до систем та більше можливостей для проникнення. Завдяки інцидентам із загрозою внутрішньої інформації, практики інсайдерів можна ідентифікувати та, отже, боротись із відповідними засобами захисту.

Висновки

Незважаючи на зростаючу потребу в методі, здатному допомагати виявляти інсайдерські загрози, на даний момент відсутній універсальний підхід, здатний комплексно вирішувати проблему виявлення внутрішніх загроз і протидії їм, тому що виявлення інсайдерської загрози можливо тільки при наявності адекватної моделі, яка описує організацію, її інформаційні активи і працівників.

Перевагою запропонованої моделі, яка базується на поєднанні двох підходів – реалізації технічного методу та психології, є її простота та зручність у використанні. Оцінки базуються на думці експертів, що дає можливість уникнути певного формалізму у порівнянні з машинним оцінюванням.

Перелік посилань

1. Omar, M. Insider Threats: Detecting and Controlling. In New Threats and Countermeasures in Digital Crime and Cyber Terrorism; IGI Global: Hershey, PA, USA, 2015; p. 162.
2. ENISA Threat Landscape 2020 - Insider threat https://www.enisa.europa.eu/publications/insider-threat
3. Compromised Insider, The Problems It Causes Organisations? Cyberseer. Available online: https://www.cyberseer.net/solutions-and-services/common-threats/compromise-insider .
4. Walker-Roberts, S.; Hammoudeh, M.; Dehghantanha, A. A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. IEEE Access 2018, 6, 25167–25177.
5. Yates, D.; Harris, A. International Ethical Attitudes and Behaviors: Implications for Organizational Information Security Policy. In Information Assurance and Security Ethics in Complex. Systems: Interdisciplinary Perspectives; IGI Global: Hershley, PA, USA, 2011; pp. 55–80.
6. Greitzer, F.L.; Frincke, D.A.; Zabriskie, M. Social/ethical issues in predictive insider threat monitoring. In Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives; IGI Global: Hershey, PA, USA, 2010; pp. 132–161.

Надійшла: 08.02.2021 Рецензент: д.т.н., професор Гайдур Г.І.