УДК 004.056
DOI: 10.31673/2409-7292.2022.036575

Заікін С.С., Іщук М.О.

МЕТОДИКА ВИБОРУ ЗАХОДІВ ПРОТИДІЇ ІНСАЙДЕРСЬКИМ ЗАГРОЗАМ В ОРГАНІЗАЦІЇ

В роботі 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 різновид 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. Зазначено, що організації можуть запровадити деякі основні заходи, які можуть зменшити кількість випадків інсайдерських загроз до мінімуму на основі поєднання формальних, неформальних та технічних заходів.

Ключові слова: Інсайдер, інсайдерська загроза, кібербезпека організації, компрометація мережевого середовища.

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.

Метою даної статті є вивчення проблеми виявлення інсайдерських загроз інформаційної безпеки та протидії їм. Для досягнення поставленої мети необхідно вирішити такі завдання: вивчити актуальну інформацію про інсайдерські загрози, виявити до чого може привести наявність таких загроз, та яким чином здійснюється протидія інсайдерським загрозам.

Класифікація підходів щодо нейтралізації або пом'якшення наслідків від інсадйреських загроз на підприємстві

Інсайдерські загрози створюють інсайдери, які використовують вразливі місця в інформаційних системах підприємства чи організації. З одного боку, заходи інформаційної безпеки можуть зменшити вразливі місця, що призводять до ризику зловживання інформацією; з іншої сторони ці ж заходи насправді можуть мати вразливі місця, що призводять до інших ризиків (ISO/IEC 15408, 1999).

Інформаційна безпека - це не тільки питання технічного контролю або заходів безпеки. Інформаційна безпека передбачає врахування наявності людей/користувачів, організаційних факторів, технологій та робочих середовищ. Щоб охопити все це було запропоновано три види контролю безпеки для ефективного забезпечення інформаційна безпеки в системах організацій та підприємств:

- Технічний контроль включає механізми захисту інформаційних систем від атак або інцидентів. Антивірусне програмне забезпечення, засоби контролю доступу, резервні копії, відновлення та аудит програмне забезпечення.
- Формальний контроль включає бізнес-структури та процеси, які забезпечують правильність загальне ведення бізнесу та зменшення ймовірності інциденту чи нападу, або принаймні мінімізувати його вплив. Наприклад, відокремлення організації безпеки від інших IT-відділів, розроблений правильний розподіл обов’язків, а отже доступ до прав та привілеїв, проектування та контроль відповідного керівника за взаємодією між працівниками, рутинна оцінка ризику тощо.
- Неформальний контроль по суті стосується культури, цінностей та системи переконань організації. Організаційна культура, в якій можна зрозуміти наміри керівництва, що сприяє виробленню спільного бачення та інших неформальних цілей, зробила б членів організації більше відданими своїй діяльності та успіху організації в цілому. Неформальний контроль може бути створений, наприклад, шляхом підвищення обізнаності про безпеку проблеми через освітні та навчальні програми.

- Індивідуальний контроль у кожній з трьох категорій, хоча і є важливим, але покликаний доповнювати один одного. Недавні дослідження підтверджують це і вказують на те, що успішний захист від інсайдерських загроз залежить як від технічного, так і від поведінкового характеру в організації.

Запобігання, виявлення та реагування на інсайдерські загрози

Окрім розмежування технічного, формального та неформального контролю, також існує класифікація заходів відносно з їх часу.

Профілактика – це заходи, спрямовані на уникнення появи інсайдерської загрози, включаючи заходи для прогнозування атак інсайдерів на основі потенційних показників. Дотримання нормативних вимог змушує організації переглянути спосіб підходу до управління ризиками; внутрішня політика є основою для дотримання нормативних актів та запобігання інсайдерським інцидентам. Політика визначає та регулює дії та поведінка персоналу в організації. Однак політика сама по собі не дуже корисна, якщо не підкріплена наслідками. Ці наслідки мають найбільший вплив на інсайдерську загрозу.

Виявлення – це заходи, спрямовані на виявлення присутності інсайдера, коли фактична атака відбувається або вже відбулася. Існує кілька методів доступних для виявлення атак. Однак виявити дії інсайдерів набагато важче. Інсайдерські дії можна виявити за допомогою інструментів для моніторингу та реєстрації, політик безпеки або повідомлень про порушення.

Сигналізація – це заходи, які застосовуються для подолання інсайдерської загрози після того як її виникнення відбулося. Ці заходи можуть бути коригуючими та репресивними, щоб мінімізувати ефект.

Категоризація заходів

Запропоновано дві класифікації заходів. Сюди входить розмежування між формальним, неформальним та технічним контролем та класифікацією, що грунтується на запобіганні, виявленні та реагуванні. На рис. 1 ці класифікації заходів поєднані з властивостями захисту інформації: конфіденційності, цілісності та доступності.

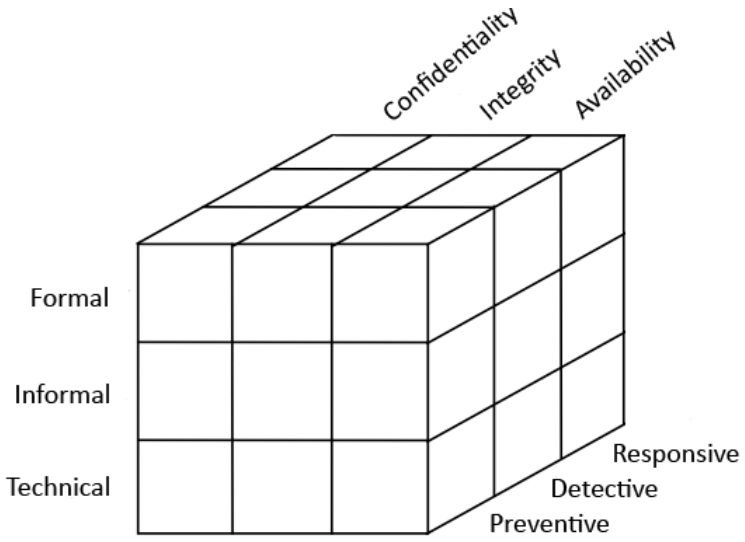

Рис. 1. Поєднання класифікації інсайдерських загроз з властивостями захисту інформації

Недавні дослідження показують, що успішний захист від інсайдерської загрози залежить від технічних та поведінковвих рішень, адже ці рішення повинні доповнювати одне одного. Цю категоризацію можна розширити, оцінивши властивості безпеки, на які впливають шляхом впровадження заходів. Деякі заходи стосуються всіх властивостей безпеки, інші - більш конкретні та стосуються, наприклад, лише конфіденційності. Організаціям та підприємствам можливо доведеться зосередитись зокрема на захисті однієї

із властивостей, оскільки, наприклад, оцінка ризику показали високі показники щодо доступності інформації. Отже, властивості захисту повинні також бути включеними до категорії заходів.

Заходи щодо пом'якшення інсайдерським загрозам представлені у табл. 1 та класифікуються на офіційні, неформальні та технічні елементи керування. Крім того, кожен із заходів пов'язаний із властивостями безпеки, що зазнають впливу. Як було зазначалося раніше, деякі заходи впливають на всі властивості безпеки, а деякі стосуються лише одного специфічне майно безпеки.

Таблиця 1

Категоризація пом’якшувальних заходів щодо властивостей захисту інформації

Заходи	Конфіденційність	Цілісність	Доступність
Формальні заходи	Політика безпеки; Скринінг працівника перед працевлаштуванням; Фізичний контроль доступу; Подвійне управління; Поділ обов'язків; Відкликання дозволів; Найменший привілей; Реєстрація інцидентів; Аудит		
	Юридично обов’язковий документи; Політика «чистого» столу; Обмеження на знімні носії	Безпека в програмному забезпеченні Розвиток життя Цикл	Непередбачені обставини планування
Неформальні заходи	Освіта в галузі безпеки; Керувати організаційною культурою		
Технічні заходи	Автентифікація; Рольовий контроль доступу; Моніторинг та реєстрація; Система виявлення вторгнень		
	Шифрування; Водяні знаки; Захист від витоку даних	Контроль додатків; Антивірус	Резервне копіювання

Побудова матриці залежості заходів протидії інсайдерським загрозам

Заходи, описані в табл. 1, перенесені до табл. 2. Ця таблиця показує чи є заходи превентивними, детективними чи реагуючими та в якій мірі вони здатні нейтралізувати чи пом'якшити інсайдерські загрози. Часовий аспект визначає фокус пом'якшення наслідків. Моніторинг і реєстрація не може, наприклад, запобігти фактичній атаці, але насправді допомагає ідентифікувати інсайдера. Більше значення приділяється заходам, які є профілактичними, порівняно з тими, які є детективними чи реагуючими. Крім того, ступінь пом'якшення також визначає обмежуваність заходів. Обмежуваність заходів полягає в тому, як інсайдер здатний обійти певну міру.

У табл. 2 наведено огляд ефективності заходів з точки зору ступеня загрози. В табл. 2 приведені певні скорочення, а саме: P – превентивний, D – детективний, R – реагуючий. 01 – Фізичний доступ для розповсюдження інформації; 02 – Фізичний доступ для перегляду інформації; 03 – Фізичний доступ до інформації про саботаж; 04 – Розкриття інформації через крадіжку; 05 – Ненавмисне знищення інформації; 06 – Зловживання мережевим доступом для розповсюдження; 07 – Зловживання мережевим доступом для зміни інформації; 08 – Зловживання мережевим доступом до інформації про саботаж; 09 – Зловживання мережевим доступом для встановлення зловмисних програм; 10 – Зловживання отриманим доступом до мережі; 11 – Зловживання невідкликаним доступом до мережі; 12 – Ненавмисний розподіл за допомогою мережі; 13 – Ненавмисне зловживання інформаційною системою; 14 – Випадкова інсталяція шкідливого програмного забезпечення; 15 – Ненавмисне використання несанкціонованого доступу; L – низький рівень пом'якшення; M – середній; H – високий ефект пом'якшення.

Більшість офіційних заходів мають низький або середній ефект пом'якшення наслідків, за винятком фізичного контролю доступу, обмежень при використанні змінних носіїв. Ці заходи є більш суворими і, отже, призводять до обмеження свободи інсайдерів підривати політику, яку описано, наприклад в політиці безпеки. Політика безпеки важлива для встановлення керівних принципів та опису належної поведінки, включаючи покарання за

невиконання певних дій, але не обмежує здатність інсайдерів представляти загрози організації. Інші заходи, такі як принцип найменших привілеїв не може перешкоджати інсайдерам, які мають відповідні повноваження в компанії зловживати цими дозволами; принцип найменших привілеїв може лише пом'якшити вплив цього зловживання.

Неформальні заходи пов'язані із спілкуванням як заходів офіційного, так і технічного характеру, та підвищення обізнаності працівників щодо теми безпеки в цілому. Хоча обізнаність щодо інформаційної безпеки здатна пом’якшити деякі загрози, в більшості випадків вона має профілактичний характер. Вона не в змозі ефективно пом'якшувати інсайдерські загрози, наприклад, зловмисними інсайдерами. Обізнаність в галузі інформаційної безпеки і управління організаційною культурою підприємства може створити лише середовище, в якому працівники знають про можливі загрози і готові повідомляти про підозрілі випадки своїх колег. Таким чином, ці заходи більше зосереджені на виявленні інсайдерських загроз.

Таблиця 2

Матриці залежості заходів протидії інсайдерським загрозам

Заходи	P	D	R	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
Політика безпеки	+		+	M	M	L	M	L	M	M	M	M	L		M		M	L
Скринінг перед працевлаштуванням	+			L	L	L			L	L	L	L	L					
Документи, що мають юридичну силу	+		+	M	L				M									
Фізичний контроль доступу	+	+		M	M	H												
Подвійне управління	+					L			L	M	M					L		
Поділ обов'язків	+									M	M					L		
Найменший привілей	+								L	L	L	L		L	L	L	L	L
Політика «чистого» столу	+			H	H	L												
Видалення обмежень. носій	+						H		H						M			
Аудит		+	+						M	M	M	M	M	M	L	L	L	L
Реєстрація інцидентів		+	+	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L
Освіта з питань безпеки	+	+		M	M	M	M						M		M		M	H
Управління орг. культура	+	+		L	L	L	L	L	L	L	L	L	L	L	L		L	L
Очистити політику екрану	+												H					
Аутентифікація	+			M	M	M			M	M	M	M	H					
Рольовий контроль доступу	+								L	L	L	L						
Антивірус	+											H					H	
Шифрування	+			M			H								H			
Водяний знак	+	+		M			M		M						M			
Моніторинг та реєстрація		+	+						M	M	M	M	M	M	M	M	L	M
Система виявлення вторгнень		+	+						L	L	L	L	L	L				
Набори для запобігання втраті даних	+	+							H						H			
Резервне копіювання			+			H		M		M	H	M				M	M	
Контроль додатків	+									M						H		

Політика «чистого» робочого столу та обмеження на використання знімних носіїв, деякі технічні заходи також призводять до обмеження свободи інсайдерів користуватися інформацією та/або інформаційними системами, які містять конфіденційну інформацію.

Методи як на фізичному, так і на логічному периметрі обмежують легкий доступ до цінної інформації і, отже, ефективніші для пом'якшення загроз. Шифрування може ефективно пом'якшувати загрози, пов'язані з розголошенням або втратою цінної інформації,

а засоби контролю додатків ефективно пом'якшують загрози, пов'язані з неправильним використанням інформації системи для зміни інформації. Хоча заходи резервного копіювання ефективні, вони реагують і таким чином, здатні оговтатися від погроз. Моніторинг та реєстрація – це важливий контроль, що дозволяє організації виявляти та розслідувати підозрілих інсайдерів, отже, це ефективний захід переслідування зловмисних інсайдерів.

Загрози, які можуть представляти особи, які мають фізичний доступ, можуть бути пом'якшені ефективно завдяки поєднанню заходів, таких як фізичний контроль доступу, політика «чистого» столу та обмеження на використання знімних носіїв. Загрози, які використовують авторизовану мережу, є більш складними для пом'якшення. Обмеження щодо використання знімних носіїв можуть обмежити можливості транспортування цінної інформації за межі організації, але інші уразливості залишаються не виявленими. Навіть із поєднанням принципу найменших привілеїв та розподілу обов'язків, уповноважені інсайдери можуть використовувати їх права доступу. Для пом'якшення цих загроз використовується комбінація моніторингу та реєстрації та рольового контролю доступу, що може бути застосований для виявлення зловживань, включаючи фактичного винного.

Отримання дозволеного доступу до мережі від іншого інсайдера за допомогою комп’ютера який залишився без нагляду або використання викрадених облікових даних користувача може ефективно пом'якшити поєднання застосування посиленої автентифікації.

Загалом, матриця заходів проти загрози показує, що лише невелика кількість кроків здатна насправді пом'якшити або мінімізувати інсайдерські загрози. Той факт, що інсайдери мають законний доступ, дає їм широкі можливості для здійснення діяльності з розповсюдженням та/або транспортуванням інформації, її зміни або навіть знищенням. Хоча такі заходи, як принцип найменших привілеїв, подвійний контроль, поділ обов'язків ефективний, однак інсайдери все ще здатні використовувати дозволи, якими вони користуються потреба в комерційних цілях. Не існує єдиного рішення внутрішньої загрози; заходи можуть застосовувати лише для зменшення ризику. Організації вживають заходів щодо зменшення ризиків для конфіденційності, цілісності та доступність інформації.

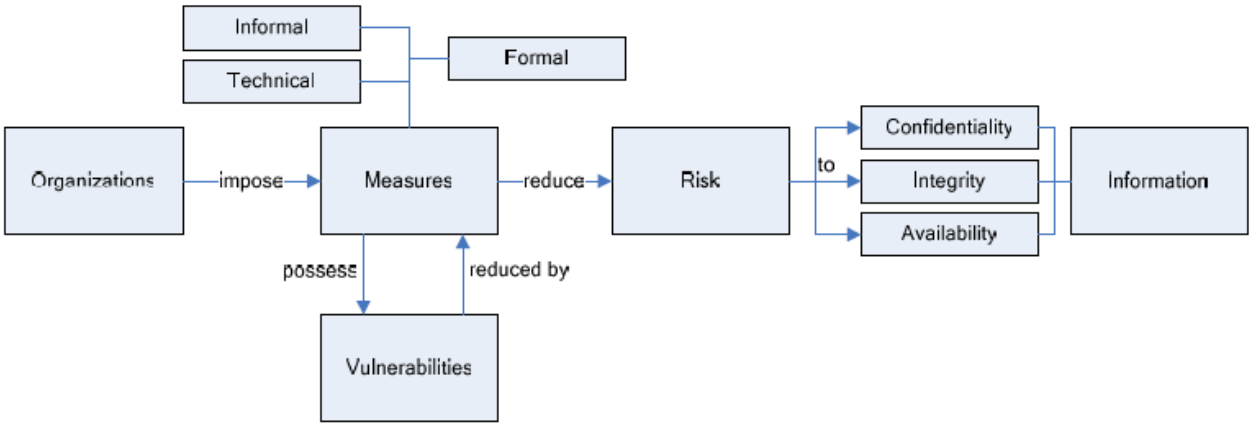

Рис. 2. Заходи щодо пом'якшення наслідків для зменшення ризиків, спричинених інсайдерами

Строгий контроль доступу та скасування дозволів може допомогти зменшити вплив внутрішньої загрози виникнення. Моніторинг та реєстрація журналу дуже важливі для виявлення зловживання та для можливості притягнути до відповідальності встановленого зловмисника. Заходи можуть лише зменшити проблему внутрішньої загрози; немає єдиного рішення для протидії інсайдерські загрози. З одного боку, заходи інформаційної безпеки зменшують вразливості, які призводять до ризиків, з іншого боку, ці заходи містять в собі інші вразливі місця, які можуть бути використані. Крім того, є, звичайно, витрати та зусилля, пов'язані з застосування заходів безпеки. Ці витрати та зусилля включають не лише

фінансові витрати на IT-ресурси, але також зниження продуктивності та креативності, а також появу недовіри між роботодавцем та працівниками. Отже, маючи або використовуючи цінну інформацію важливо враховувати тей факт, що вона повинна не перевищувати витрати на здійснення заходів, які потребують її захисту.

Висновки

Розглянуто сучасні підходи та засоби контролю, пов'язані зі зменшенням рівня інсайдерських загроз. Підкреслено, що не існує єдиного рішення, яке могло б повністю усунути внутрішню загрозу в організації. Крім того, технічний підхід сам по собі може бути не найефективнішим способом запобігання та виявлення зловмисних внутрішніх загроз. Зроблено висновок, що жоден єдиний підхід не може вирішити проблему безпеки. З метою пом'якшення внутрішньої загрози необхідні додаткові дослідження в галузі внутрішніх загроз кібербезпеки, і слід визначити правильний підхід до боротьби зі зловмисною внутрішньою загрозою з різних точок зору. Зазначено, що організації можуть запровадити деякі основні заходи, які можуть зменшити кількість випадків інсайдерських загроз до мінімуму. Бажано здійснити багаторівневий захист формальних, неформальних та технічних заходів.

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. Insider Threat, Imperva. Available online: https://www.imperva.com/learn/application-security/insider-threats (accessed on 7 May 2020).
3. Compromised Insider, The Problems It Causes Organisations? Cyberseer. Available online: https://www. cyberseer.net/solutions-and-services/common-threats/compromise-insider .
4. Clark J.; Leblanc S.; Knight S. Risks associated with USB hardware Trojan devices used by insiders. In Proceedings of the IEEE International Conference on Systems Conference (SysCon), Montreal, QC, Canada, 4–7 April 2011; pp. 201–208.
5. Potts M. Internal Network Visibility for APTs and Insider Threats. Lancope, Inc.: Alpharetta, GA, USA, 2016. Available online: https://www.insightssuccess.com/lancope-preeminent-network-visibility-and-security-intelligence/
6. Ray L.; Felch H. Detecting advanced persistent threats in oracle databases: Methods and techniques. In Strategic Information Systems and Technologies in Modern Organizations; IGI Global: Hershey, PA, USA, 2017; pp. 71–89.
7. Scott J.; Spaniel D. In 2017, The Insider Threat Epidemic Begins. Institute for Critical Infrastructure Technology, February 2017. Available online: https://icitech.org/wp-content/uploads/2017/02/ICIT-Brief-In- 2017-The-Insider-Threat-Epidemic-Begins.pdf
8. Iyer R.; Dabrowski P.; Nakka N.; Kalbarczyck Z. Pre-configurable tamper-resistant hardware support against insider threats: The tested ILLIAC approach. In Insider Attack and Cyber Security; Springer: New York, NY, USA, 2008; pp. 133–152.
9. Greitzer F.L.; Strozer J.R.; Cohen S.; Moore A.P.; Mundie D.; Cowley J. Analysis of unintentional insider threats deriving from social engineering exploits. In Proceedings of the IEEE Security and Privacy Workshops, San Jose, CA, USA, 17–18 May 2014; pp. 236–250.
10. CERT. Insider Threat Control: Using a SIEM Signature to Detect Potential Precursors to IT Sabotage. Carnegie Mellon University, Software Engineering Institute: Pittsburgh, PA, USA. Available online: https://insights.sei.cmu.edu/insider-threat/2012/01/insider-threat-control-using-a-siem-signature-to-detect-potential-precursors-to-it-sabotage.html
11. 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.
12. Brdiczka O.; Liu J.; Price B.; Shen J.; Patil A.; Chow R.; Bart E.; Ducheneaut N. Proactive insider threat detection through graph learning and psychological context. In Proceedings of the 2012 IEEE Symposium on Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24–25 May 2012; pp. 142–149.

Надійшла: 09.09.2022 Рецензент: д.т.н., професор Кожухівський А.Д.