Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
« » червня 2021р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Інсайдерські атаки, методи їх запобігання та протидії»

Виконавець: студент IV курсу, групи КБ-41

_____ **Мухайдлі Шаді-Олександр Рабіанович**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Браіловський М.М.	

Нормоконтроль	Даков С.Ю.	

Київ 2021

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«10» жовтня 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-41** (група) **Мухайдлі Шаді-Олександру Рабіановичу** (прізвище ім'я по-батькові)

Тема дипломної роботи Інсайдерські атаки, методи їх запобігання та протидії

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2020 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Методи захисту від інсайдерськоих атак

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно проаналізувати методи захисту від інсайдерських атак,
провести аналіз програмних рішень для тих чи інших методів захисту

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рекомендації щодо методів захисту від інсайдерських атак та проаналізовано відповідні програмні рішення.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання:12 жовтня 2020 року

Завдання видав		М.М. Браіловський
	(підпис)	(ініціали, прізвище)
Завдання прийняла до виконання		Ш.-О.Р. Мухайдлі
	(підпис)	(ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Вивчення літератури	15.10.2020 – 21.02.2021	*виконано*
2	Написання загального плану роботи	22.02.2021 – 01.03.2021	*виконано*
3	Написання першого розділу дипломної роботи	02.03.2021 – 31.03.2021	*виконано*
4	Написання другого розділу дипломної роботи	01.04.2021 – 18.04.2021	*виконано*
5	Проходження переддипломної практики	19.04.2021 – 07.05.2021	*виконано*
6	Написання третього розділу дипломної роботи	12.05.2021 – 27.05.2021	*виконано*
7	Підготовка до захисту дипломної роботи	28.05.2021 – 08.06.2021	*виконано*

Завдання видав		М.М. Браіловський
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання		Ш.-О.Р. Мухайдлі
	(підпис)	(ініціали, прізвище)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 68 сторінок основного тексту, 3 рисунка. Список використаних джерел містить 52 найменування і займає 4 сторінки.

Метою даної роботи є аналіз інсайдерської загрози, визначення методів її виявлення, запобігання та протидії.

У роботі визначені основні терміни для розуміння подальшого контексту, такі як: інсайдерська інформація, інсайдери, інсайдерська загроза згідно нормативно-правовій базі.

У роботі було проаналізовано статистику кількості інсайдерських атак, які групи працівників найчастіше можуть стати інсайдерами, проведено аналіз впливу інсайдерської загрози на установи та організації.

Досліджено основні способи протидії інсайдерській загрозі , такі як: моніторинг користувачів, запобігання втраті даних, аналіз поведінки користувачів та організацій та розроблено рекомендації щодо програмних рішень для них.

Ключові слова: інсайдерська інформація, інсайдер, інсайдерська загроза, моніторинг користувачів, АПКО.

ЗМІСТ

ВСТУП

Актуальність роботи. У суспільстві, де кожен громадянин оснащений високотехнологічними гаджетами, що дозволяють отримувати, зберігати та обробляти інформацію з нечуваною раніше швидкістю, інсайдерська загроза – це найбільший щоденний ризик безпеки інформації, з яким стикаються люди, змушені працювати з конфіденційною інформацією. При цьому, як не дивно, усвідомлення ролі інсайдерських загроз часто призводить до почуття хибної впевненості у розумінні проблеми та захищеності від неї.

І, хоча число шкідливих інсайдерів вважається незначним, істотні ризики для безпеки підприємств залишаються через можливість ненавмисних вторгнень, кількість яких дедалі збільшується. Інсайдерські загрози виходять від внутрішніх користувачів, які мають достатні права доступу, можуть ефективно маскуватися та приховувати свою діяльність, ускладнюючи можливість їх виявлення та запобігання загрозам. Ризик збільшується через швидкий розвиток хмарних обчислень, необхідність формування та підтримування великих обсягів даних, застосування технологій централізованої їх обробки. Тому, з метою зменшення втрат, що можуть спричинити інсайдерські загрози, двома найважливішими питаннями в галузі інформаційної безпеки стали виявлення та упередження інсайдерських загроз.

Метою роботи є аналіз інсайдерської загрози, визначення методів її виявлення, запобігання та протидії.

Для досягнення мети поставлені завдання:

- Визначити значення основних термінів, таких як інсайдерська інформація, інсайдери, інсайдерська загроза згідно нормативно-правовій базі;
- Провести статистичний аналіз кількості інсайдерських атак, визначити які групи працівників найвірогідніше стають інсайдерами, провести аналіз впливу інсайдерської загрози на установи та організації;
- Дослідити основні напрями виявлення інсайдерів;
- Дослідити основні напрями запобігання інсайдерським атакам;

- Визначити основні практичні способи виявлення, запобігання та протидії інсайдерській загрозі.

Об'єкт дослідження – вплив інсайдерської загрози, процес дослідження методів її запобігання.

Предмет дослідження – методи захисту від інсайдерських атак.

Методи дослідження. У роботі були використані такі загальнотеоретичні методи як аналіз, синтез, метод абстрагування та індукції.

Практичне значення: Результати дослідження можуть бути використані компаніями для забезпечення захисту від інсайдерських атак; у навчальному процесі Київського національного університету імені Тараса Шевченка при підготовці навчальних дисциплін за спеціальністю 125 «Кібербезпека».

РОЗДІЛ 1
ОСНОВНІ ТЕРМІНИ І ПОНЯТТЯ

Для того щоб розглянути сутність проблеми спершу потрібно розібрати основні поняття, такі як:

1. Інформація з обмеженим доступом
2. Інсайдерська іформація
3. Інсайдерська торгівля
4. Інсайдер
5. Інсайдерська загроза

1.1 Інформація з обмеженим доступом

Необхідні поняття були розглянуті в законі України «ПРО ДОСТУП ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ»[1]:

Інформація з обмеженим доступом - це інформація, до якої має доступ тільки обмежена кількість осіб і розкриття якої заборонено відповідно до закону. Обмеження доступу до інформації здійснюється в інтересах національної безпеки або захисту законних прав фізичних та юридичних осіб. Доступ до інформації обмежений, а не до документу. Відповідно, якщо один документ містить відкриту і закриту інформацію, перша може бути надана зацікавленій особі у вигляді окремого документа.

Доступ до інформації може бути обмежений, якщо:

- обмеження здійснюється виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для захисту здоров'я населення, для захисту репутації або прав інших осіб, для запобігання розголошенню конфіденційної інформації або підтримки авторитет і неупередженість правосуддя. ;
- розголошення інформації може завдати значної шкоди цим інтересам;

• збиток від розкриття такої інформації переважає суспільний інтерес в її отриманні.

Інформація є обмеженою, а не документ. Якщо документ містить обмежену інформацію, необмежена інформація надається для ознайомлення.

Інформація з обмеженим доступом включає конфіденційну, офіційну та секретну інформацію.

Будь-яка інша інформація вважається відкритою, і всі громадяни України мають право на доступ до неї, незалежно від того, стосується ця інформація їх безпосередньо чи ні.

Конфіденційна інформація - інформація про фізичну чи юридичну особу, доступ і поширення якої можливі тільки за згодою її власників (тих, до кого ця інформація відноситься безпосередньо) і на зазначених ними умовах.

Конфіденційна інформація юридичної особи.

Ця інформація міститься в договорах, угодах, листах, звітах, аналітичних матеріалах, бухгалтерських звітах, графіках, графіках, специфікаціях та інших документах, які фігурують в діяльності юридичної особи. Розкриття даних, що містяться в таких документах, може бути використано конкурентами і, відповідно, завдати економічної та іншої шкоди юридичній особі.

Конфіденційна інформація про людину:

Конфіденційна інформація про людину включає, крім іншого, інформацію про його або її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адресу, дату і місце народження. Збір, зберігання, використання та поширення конфіденційної інформації про особу без її згоди не дозволяється, за винятком випадків, передбачених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини.

1.2 Що таке інсайдерська інформація?

Необхідні поняття були розглянуті у Законі України "Про цінні папери та фондовий ринок"[2]:

Інсайдерська інформація - неоприлюднена інформація про емітента, його цінні папери та похідні (деривативи), що перебувають в обігу на фондовій біржі, або правочини щодо них, у разі якщо оприлюднення такої інформації може істотно вплинути на вартість цінних паперів та похідних (деривативів), та яка підлягає оприлюдненню відповідно до вимог, встановлених законом.

Обмежена кількість людей всередині компанії неминуче дізнається про подію, яка, як тільки вона буде виявлена, істотно вплине на курс акцій компанії. Це може бути незавершене злиття, відгук продукту, недоотриманий прибуток або провал великого проекту. В крайньому випадку, це може бути фінансовий скандал, який ось-ось стане надбанням громадськості.

Знаючим людям заборонено законом використовувати ці знання, купуючи або продаючи акції компанії або передаючи інформацію комусь іншому, хто нею користується.

Інсайдерська торгівля є незаконною, якщо інформація не була оприлюднена і використовувалася для обміну. Це розглядається як несправедливе маніпулювання вільним ринком з метою надання переваг певним сторонам. В кінцевому підсумку це підриває впевненість в цілісності ринку та може уповільнити економічне зростання.

1.3 Інсайдерська торгівля

Інсайдерська торгівля - це торгівля акціями публічної компанії чи іншими цінними паперами (наприклад, облігаціями чи опціонами на акції) на основі суттєвої, непублічної інформації про компанію. У різних країнах деякі види торгівлі на основі інсайдерської інформації є незаконними. Це пояснюється тим, що це вважається несправедливим щодо інших інвесторів, які не мають доступу до інформації, оскільки інвестор, що має інсайдерську інформацію, потенційно може отримати більший прибуток, ніж типовий інвестор. Правила, що регулюють торгівлю інсайдерами, є складними і суттєво різняться залежно від країни. Ступінь правозастосування також варіюється в залежності від країни. Визначення інсайдера

в одній юрисдикції може бути широким і може охоплювати не тільки самих інсайдерів, але й будь-яких пов’язаних з ними осіб, таких як брокери, партнери та навіть члени родини. Особа, якій стало відомо про непублічну інформацію та торгує на цій основі, може бути винною у скоєнні злочину.

Незаконна інсайдерська торгівля

Більш сумнозвісною формою інсайдерської торгівлі є незаконне використання непублічної матеріальної інформації з метою отримання прибутку. Важливо пам’ятати, що це може робити будь-хто, включаючи керівників компаній, їхніх друзів та родичів, або просто звичайну людину на вулиці, якщо інформація не відома публічно.

Наприклад, припустимо, що генеральний директор фірми ненавмисно розкриває щоквартальні прибутки своєї компанії під час стрижки. Якщо перукар користується цією інформацією та торгує нею, це вважається незаконною інсайдерською торгівлею.

Інсайдерська інформація - це знання матеріалів, пов’язаних із публічною компанією, що забезпечує несправедливу перевагу для торгівця чи інвестора. Наприклад, скажімо, віце-президент інженерного департаменту технологічної компанії підслуховує зустріч між генеральним директором та фінансовим директором

За два тижні до того, як компанія показала свої прибутки, фінансовий директор повідомляє генеральному директору, що компанія не відповідає очікуванням продажів і втратила гроші за останній квартал. Віце-президент інженерного департаменту знає, що його друг володіє акціями компанії, і попереджає друга, щоб він негайно продав їх акції . Це приклад інсайдерської інформації, оскільки заробіток не оприлюднювався.

Припустимо, друг віце-президента продає їхні акції та виставляє 1000 акцій до виходу прибутку. Тоді це незаконна інсайдерська торгівля. Однак, якщо вони торгують цінним папером після оприилюднення заробітку, це не вважається незаконним, оскільки вони не мають прямої переваги над іншими трейдерами чи інвесторами.

1.4 Інсайдери

Інсайдер це:

- будь-яка особа (юридична або фізична), яка має доступ до конфіденційної інформації про діяльність фірми в силу свого службового становища або сімейних зв'язків;
- особа, яка в силу свого положення має доступ до важливої (фінансової) інформації, недоступною для широкого загалу. Операції з інсайдерськими акціями строго контролюються, реєструються і публікуються;
- особа, яка володіє більше 10% акцій товариства (підприємства, заводу і т. Д.).

Інсайдер, що володіє інформацією «з внутрішніх джерел», може краще оцінити стан справ, ніж будь-який інший фахівець, який використовує «зовнішню» інформацію для експертного висновку.

Інсайдерами не народжуються, інсайдерами стають.

Є декілька типів людей що можна вважати інсайдерами:

Недбалий інсайдер. Цей тип інсайдерів найчисленніший. Зазвичай це звичайний внутрішній працівник, який мимоволі порушує вимоги конфіденційності інформації.

Таким чином, у діях цього типу інсайдерів не може бути вигоди, умислу чи мети. Це безпідставно порушує вимоги конфіденційності інформації. Іншими словами, такі правопорушники можуть брати інформацію з офісу компанії, щоб працювати з нею вдома або у відрядженні. Для захисту від таких інсайдерів достатньо простих технічних засобів запобігання каналам витоку інформації: пристроїв введення-виведення інформації та фільтрації вмісту вихідного трафіку.

Маніпульований інсайдер. Такі інсайдери найчастіше стають жертвами соціальної інженерії. Ці методи використовуються не лише для незаконного отримання особистої інформації користувачів, їх паролів, номерів кредитних карток тощо.

Приклад: Працівник отримує телефонний дзвінок від майбутнього директора філії, який представляється дуже впевнено та дуже правдоподібно описує проблему неможливості доставити внутрішню пошту (тимчасові технічні труднощі). Він просить надіслати йому деяку інформацію (скажімо, фін ансові прогнози на наступний рік) у свою особисту поштову скриньку. А через кілька хвилин запитувана інформація надсилається на вказану адресу, яка є суворо конфіденційними даними. Хоча працівник діяв лише з добрими намірами, шкода від його дій, а також від дій необережних інсайдерів може бути не меншою, ніж від промислового шпигунства. Найкращий захист від таких інсайдерів - створення ситуації, коли вони не можуть порушити правила зберігання та розповсюдження інформації, зіткнувшись з технічною блокадою таких спроб. У такій ситуації як недбалі, так і маніпульовані інсайдери можуть звернутися за допомогою до колег або системного адміністратора, який вкаже їм, що неможливо і заборонено виконувати задумані дії.

Ображений інсайдер. Такі інсайдери - зловмисники, які діють переконливо і обдумано, знаючи про негативні наслідки своєї діяльності. Їх розрізняють залежно від мотивів вчинених ними ворожих дій. Так, ображений інсайдер - це працівник компанії, який розкриває конфіденційну інформацію, щоб помститися компанії з особистих причин. Більше того, ці мотиви можуть бути різними - від образи директора компанії, який в черговий раз не підняв працівника на посаду, і до елементарної відсутності моральної мотивації працювати на благо компанії.

Такого інсайдера можна визначити з двох причин:

1) він не має наміру залишати компанію;

2) його метою є заподіяння шкоди, а не крадіжка інформації як такої.

Таким чином, ці інсайдери діють таким чином, що керівництво компанії не усвідомлює, що інформація була викрадена ними. Тому, стикаючись із технічним бар'єром, який запобігає крадіжці інформації, інсайдер, як правило, спрямовує свою руйнівну силу на якийсь інший об'єкт, наприклад, на викрадення майна компанії чи фальсифікацію чи знищення доступної інформації. Важливо також, щоб ображений інсайдер, викрадаючи інформацію, виходив із власних міркувань щодо її важливості

та значення для компанії. Визначаючи адресата, якому слід передавати викрадену інформацію, ображені інсайдери часто обирають пресу або якісь тіньові структури. Водночас розкриття інформації та подальший шантаж - це головна мета, яку вони переслідують.

Нелояльні інсайдери - це працівники, які найближчим часом планують змінити свою поточну роботу. Саме ці співробітники піддаються підозрі в першу чергу, коли йдеться про внутрішні загрози. Як показала практика, сім з десяти співробітників беруть частину інформації, яка їм доступна, коли вони виїжджають, будь то клієнтська база або фінансова база. Крадіжки інтелектуальної власності також досить поширені у високотехнологічних компаніях. В основному це стажери з інших країн або тимчасові працівники. Їхні загрози не цілеспрямовані, оскільки вони часто навіть не підозрюють про цінність інформації і не знають, як і де вони можуть її використовувати. Найчастіше порушники отримують доступ до конфіденційної інформації, імітуючи потребу у виробництві, що, в свою чергу, може призвести до їх розкриття. Вкравши інформацію, вони не прагнуть приховати цей факт. У деяких випадках така інформація є гарантією зручного звільнення з відповідною компенсацією та рекомендаційними листами.

Нелояльні та невдоволені інсайдери можуть легко отримати спонукання ззовні. Ця метаморфоза відбувається, коли вони знаходять потенційного покупця конкретної інформації, це може бути преса, конкуренти або кримінальні структури.

Інсайдер що отримує гроші за свою роботу. Ситуація з нелояльними і скривдженими інсайдерами кардинально змінюється, якщо вони раніше зв'язалися з покупцем з інформацією, необхідної для крадіжки. Головна відмінність буде в цілях: підроблені і вбудовані інсайдери - це буде бажання заробити на передачі інформації. У деяких випадках від правильності «роботи» буде залежати власне життя і здоров'я. Підроблені та вбудовані інсайдери не власними визначають мету крадіжки інформації, це робить за них потенційний замовник.

Мотивувати таких інсайдерів можна з різних причин: від бажання заробити грошей на довгоочікувану покупку, до примусу, коли таких співробітників шантажують певні структури і їм нічого не залишається, окрім як вкрасти

конфіденційну інформацію. В крайньому випадку, такі співробітники можуть навіть піти на хабар іншим співробітникам компанії або зламати, щоб отримати необхідну інформацію.

Засланий інсайдер. Щоб краще зрозуміти, хто такий вбудований співробітник, наведемо приклад. Системного адміністратора однієї з процвітаючих компаній несподівано надходить пропозиція про перехід на нову роботу. Пропозиція настільки заманливо, що відмовитися від нього просто неможливо, адже зарплата, соціальні гарантії та графік роботи такі, що нічого кращого не придумаєш. При цьому поки системний адміністратор збирає свої речі, в відділ кадрів надходить блискуче резюме не менше блискучого співробітника того ж профілю і спеціальності. Відмовитися від цього фахівця теж не можна, тим більше що він з'явився саме вчасно. Таким чином, новий співробітник легко і в короткі терміни отримує доступ до конфіденційної інформації і передає її своєму замовнику, після чого цей системний адміністратор, природно, зникає. В результаті компанія втрачає свої корпоративні секрети, а справжній системний адміністратор, розкльовувати привабливу пропозицію, взагалі залишається без роботи. Основна небезпека, яку представляють вбудовані інсайдери, полягає в тому, що їм надаються необхідні технічні навички, що дозволяють їм долати всі технічні перешкоди на шляху до отримання конфіденційної інформації.

Інсайдери та соціальна інженерія

Говорячи про інсайдерів, не можна обійти увагою використання прийомів соціальної інженерії. Дуже часто їх використання видає ідеї інсайдера - і тому дуже важливо вчасно помітити і розпізнати використання таких прийомів.

Щоб використовувати прийоми соціальної інженерії по відношенню до конкретного співробітника, инсайдеру потрібна попередня підготовка, яка дозволить йому стати ближче до своєї майбутньої жертви. Для цього йому необхідна досить докладна інформація про власника доступу до цікавлять його конфіденційних даних - включаючи інформацію про сім'ю, попередній роботі, освіті. Вираз інтересу до всієї такої інформації може свідчити про те, що витік інформації з організації готується співробітником, який проявляє подібний інтерес.

Не варто забувати і про такі близькі до соціальної інженерії інструментах, як банальні кейлоггери, які передають зловмисникові інформацію про логіни і паролі, які використовуються співробітниками, які мають доступ до конфіденційної інформації. Щоб запобігти подібні виверти з боку інсайдерів, необхідно використовувати якісне антивірусне програмне забезпечення, яке буде протидіяти роботі кейлогерів на робочих місцях користувачів.

1.5 Інсайдерська загроза

Інсайдерську загрозу можна визначити коли поточний або колишній працівник, підрядник чи інший бізнес партнер, який має або мав санкціонований доступ до мережі, системи чи даних організації та навмисно неправомірне використання, що доступ до негативно впливає на конфіденційність, цілісність або доступність організації інформація або інформаційні системи. Інсайдерські загрози, включаючи саботаж, крадіжки, шпигунство, шахрайство та конкурентні переваги часто здійснюються через зловживання правами доступу, крадіжку матеріалів та неправильне поводження з фізичними пристроями. Інсайдери не завжди діють поодинці і, можливо, не усвідомлюють, що допомагають зловмиснику.

Запобігання інсайдерським загрозам – чому це складно?

Через характер внутрішньої загрози їх практично неможливо повністю запобігти. Працівник, який має законний доступ до конфіденційних даних, може в якийсь момент часу стати внутрішньою загрозою. Найкращий спосіб мінімізувати потенційну поверхню атаки - це діяти за політикою найменших привілеїв, коли користувачі мають доступ лише до даних, необхідних для виконання своєї роботи.

Виявлення інсайдерської загрози – чому це складно?

Інсайдерські загрози автоматично важче виявити, оскільки вони можуть просто виглядати так, наче ваші працівники виконують свою роботу як звичайно. Колишній співробітник, використовуючи свої старі облікові дані для входу та копіювання файлів та папок, до яких вони мають доступ, не буде викликати жодних

хвилювань. Інсайдерські загрози, подібні до цієї, часто можуть виявлятися роками не виявленими та наносити серйозні збитки.

Найкращий спосіб виявити внутрішню загрозу - це відстежувати поведінку користувачів та генерувати сповіщення, коли виявляється аномальна активність.

1.6 Вплив інсайдерських атак

Для того щоб зрозуміти величину впливу інсайдерських атак проаналізую дослідження cybersecurity insiders за 2020 рік.

Основними тезами є:

- 68% організацій відчувають себе середньою чи надзвичайною вразливістю до атак інсайдерів;
- 68% організацій підтверджують, що атаки з боку інсайдерів стають все частішими;
- 53% організацій вважають, що виявляти атаки інсайдерів стало складніше з моменту переходу до хмари;
- 63% організацій вважають, що привілейовані користувачі або адміни становлять найбільший ризик для внутрішньої безпеки організації.

На рисунку 1.1 викладено порівняння статистики запобігання внутрішніх атак із зовнішніх. Виявляється, більшість організацій (52%) підтверджують що внутрішні атаки важче виявити та запобігти, ніж зовнішні. Оскільки, інсайдери мають затверджені привілеї доступу, іноді буває складно відрізнити випадки законного використання матеріалів від зловмисних намірів.

Натомість 38% організацій можуть стверджувати що запобігання внутрішнім і зовнішнім атакам знаходиться на одному рівні.

І лише в 10% випадків респонденти вважають що запобігати зовнішнім атакам простіше ніж внутрішнім.

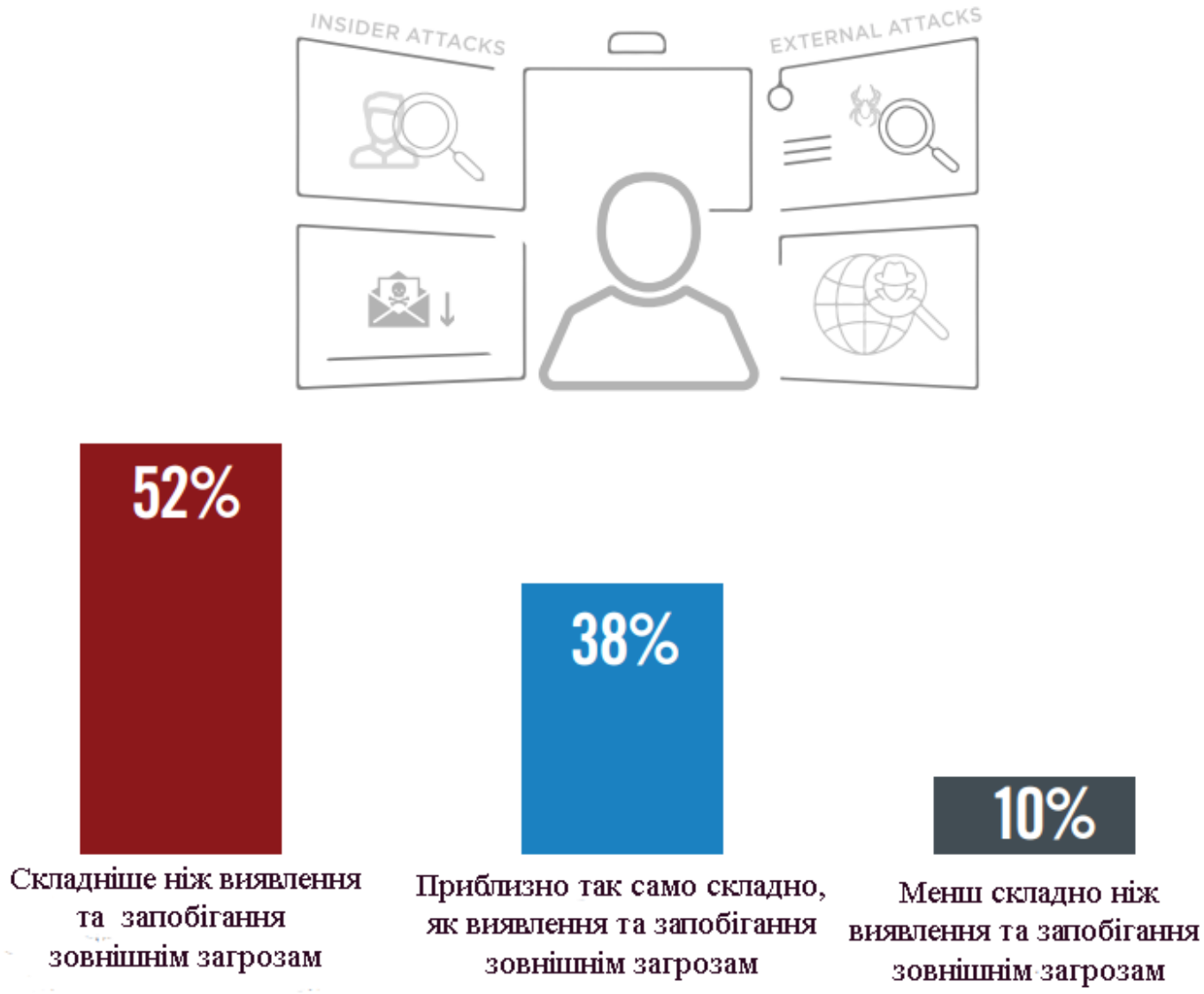

Рисунок 1.1 – Порівняння складності виявлення інсайдерських і зовнішніх атак

На наступному рисунку видно які типи інсайдерів становлять найбільший ризик для безпеки організацій.

З цього можна зробити висновок що привілейовані IT-користувачі/ адміністратори (63%) найчастіше стають інсайдерами, поряд з постійними працівниками (51%), підрядниками/постачальниками послуг/тимчасовими працівниками (50%) і керівниками (50%).

Натомість вище керівництво (16%), клієнти (15%) і бізнес партнери (11%) найрідше стають причиною витоку інсайдерської інформації.

Рисунок 1.2 – Які групи працівників найчастіше стають інсайдерами.

З наступної статистики (рисунок 1.3), можна зробити висновок, що вісімдесят сім відсотків організацій загалом вважають, що дуже важко або помірно важко визначити фактичний збиток від інсайдерських атак. І лише тринадцять відсотків можуть сказати, що вони є захищеними від інсайдерів.

Рисунок 1.3 – Наскільки складно визначити фактичну шкоду внаслідок інсайдерської атаки у організації.

Водночас, якщо порівняти дослідження 2020 року з дослідженням 2019 роком (рисунок 1.4), то оскільки інсайдери часто мають привілеї доступу до конфіденційних даних та програм, це робить важчим виявлення зловмисної діяльності у 59%. У поєднанні з розповсюдженням програм обміну даними (50%) і збільшенням даних, що залишають традиційний мережевий периметр (47%), запобігати успішним інсайдерським атакам стає все складніше.

Рисунок 1.4 – Що ускладнює виявлення та запобігання інсайдерським атакам у порівнянні з 2019 роком.

Також ускладнює виявлення інсайдерських атак пандемія, а саме перехід більшості організацій на дистанційну роботу, збільшення переносу даних у хмару, проблеми з автентифікацією пристроїв у мережі, а також людська недбалість.

Виходячи з даних, зображених на рисунку 1.5, більшість організацій (68%) зауважили, що кількість атак інсайдерів зросла протягом останніх 12 місяців. Насправді близько 70% організацій пережили одну або кілька інсайдерських атак за останні 12 місяців.

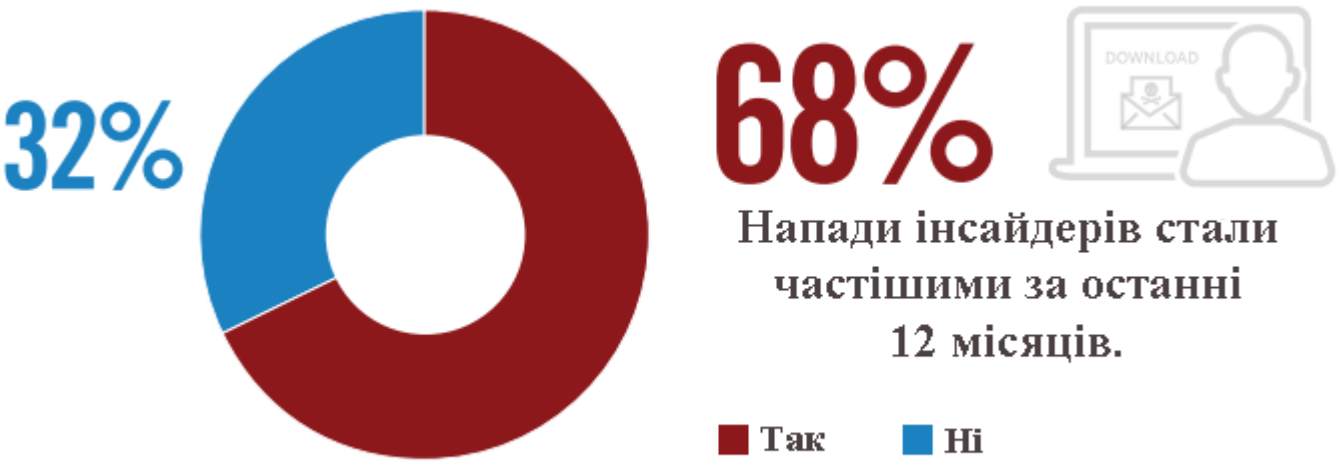

Рисунок 1.5 - Чи стали атаки інсайдерів частішими за останні 12 місяців.

Висновки до розділу 1

У розділі було розглянуто основні терміни та поняття:

- Інформація з обмеженим доступом;
- Інсайдерська інформація;
- Інсайдерська торгівля;
- Інсайдери;
- Інсайдерська загроза.

Також було проаналізовано нормативно-правову базу. Проведено аналіз частоти інсайдерських атак, кількості завданої шкоди, визначено які групи працівників становлять найбільшу загрозу для організації. Це потрібно для кращого розуміння термінології та масштабу інсайдерської загрози.

РОЗДІЛ 2
НАПРЯМИ ПРОТИДІЇ ІНСАЙДЕРСЬКИМ АТАКАМ

Ще до пандемії, працівники, незадоволені власним положенням у компанії, могли докласти зусиль для крадіжки інсайдерської інформації. Коли коронавірус потрапив у наше повсякденне життя, ця місія стала простішою. Кіберзлочинці, які зазвичай націлені на добре захищене корпоративне середовище, зараз полюють на домашні офіси, яким часто бракує надійного захисту.

Однією з нинішніх найбільш популярних шахрайських схем є видавання себе за експерта з питань охорони здоров'я чи державного агентства та спрямування користувачів на фішингові сайти про пандемію. Зловмисники реєструють домени, використовуючи такі слова, як "COVID", "коронавірус", "N95" або "маски". Вони також застосовують ці терміни в темах електронної пошти або назвах файлів, щоб отримати кліки. Потрібно лише щоб один нічого не підозрюючий користувач відкрив повідомлення, і вся система вже у небезпеці.

Ці загрози не зникнуть найближчим часом, і підприємства, які не пристосуються до цієї мінливої реальності, все частіше потрапляють у подібні інциденти. І найголовніше що вони повинні зробити, це навчити своїх працівників правильним методам запобігання, виявленню та захисту від інсайдерських атак.

2.1 Управління внутрішніми загрозами

Управління внутрішніми загрозами (Insider threat management) – це процес запобігання, боротьби, виявлення та контролю за працівниками, віддаленими постачальниками та підрядниками для укріплення даних організації від внутрішніх загроз, таких як крадіжки, шахрайство та збитки.

2.1.1 Моніторинг активності користувачів

Моніторинг активності користувачів є одним із основ будь-якої системи управління внутрішніми загрозами. Отже, навіщо моніторинг користувачів? Звичайно, співробітники не люблять бути включеними до профілю загроз власної організації, і це може бути однаково незручно з боку управління. “Нагляд” 24/7 на робочому місці також є спірним рішенням сам по собі, чи відстеження електронної пошти, журнали активності або історії пошуку в інтернеті.

Однак боротьба із загрозами всередині підприємства неможлива без цього. Це може викликати кілька складних питань, але програми моніторингу користувачів необхідні.

По-перше, організації повинні постійно перевіряти поведінку співробітників в Інтернеті, шукаючи дивні діяльності. Аналітика даних корисна в цьому відношенні. Якщо ви спостерігаєте будь-які відхилення, наприклад, підключення до невідомих або іноземних IP-адрес, про ці випадки слід позначити та повідомити. Те саме стосується випадків, коли працівники входять в систему віддалено; якщо бухгалтер, який ніколи не працює вдома, починає надсилати запити на дані посеред ночі, можливо, щось не так.

Відділ з безпеки також повинен стежити за дивними завантаженнями та передачею файлів, особливо за користувачами, які мають доступ до конфіденційної корпоративної інформації (тобто секретних даних, фінансових даних або документів про інтелектуальну власність). Розслідуючи ці інциденти та визначаючи їх причини, використовуйте цю інформацію для покращення моніторингу та аналітики.

Обсяги діяльності також можуть надати цінну інформацію. Безумовно, це правда, що деякі користувачі можуть працювати віддалено або відвідувати дивні IP-адреси як частину своєї роботи. Але раптове чи різке збільшення самої цієї діяльності (наприклад, надмірне друкування, завантаження файлів та доступ поза робочим часом) повинно насторожити. І знову ж, моніторинг повинен виконуватись із поєднання технічної та людської роботи. Наприклад, якщо ви встановили

обмеження для друку, про який знають співробітники, то спостерігачу повинно здатись дивним, що працівник друкує щось щоночі.

Звичайно, весь цей моніторинг не надто корисний без можливостей швидкого реагування. Можливість швидко розірвати IP-з'єднання, заблокувати облікові записи та закінчити передачу файлів в середині виконання - все це важливо для не просто виявлення, а й запобігання інсайдерських загроз у режимі реального часу.

Крім того, критично важливо задокументувати будь-які докази внутрішньої загрози, зібрані в рамках цього моніторингу. Для того, щоб притягнути працівника до відповідальності у суді, потрібно мати чіткі, прискіпливо збережені докази.

2.1.2 Технічна складова

Хоча моніторинг поведінки є життєво важливим для боротьби з інсайдерськими загрозами, він не може працювати сам по собі – системи, додатки, дані, пристрої та інші цифрові послуги повинні бути технічно захищені та контролюватися також від зловмисної інсайдерської діяльності. Це створює низку проблем.

Традиційні захисні механізми не дуже ефективні проти інсайдерів. Брандмауери, системи виявлення вторгнень та багатофакторні стандарти автентифікації позбавлені сенсу проти супротивника, який має активний та законний доступ до систем та інформації. Вони вже знаходяться в межах, встановлених звичайним програмним забезпеченням для безпеки, що збільшує ймовірність проскакування крізь щілини та заподіяння значної шкоди.

Крім того, навіть якщо ми і спостерігаємо за діяльністю в обліковому записі користувача, існують труднощі у розрізненні нормальної та ненормальної поведінки. Цілісність файлів є критично важливою для справжньої поінформованості про ситуацію в мережі. Якщо зашифрований файл читається десятки разів на день командою бухгалтерів, чи помітить система, якщо хтось, хто не входить до бухгалтерії, дешифрує файл? А як щодо зловмисного інсайдера в бухгалтерії - чи буде він виявлений? Як ми будемо розрізняти законні передачі

файлів та нелегітимні? А як щодо законного використання USB-накопичувачів (тобто резервного копіювання презентацій для відрядження) проти зловмисного (тобто встановлення шкідливого програмного забезпечення на корпоративні системи)?

Продовжуючи в цьому напрямку, ідеальні політичні рішення цих проблем можуть бути недоцільними. Наприклад, може бути зручно заблокувати всі завантаження в інтернеті, включаючи вкладення електронної пошти, то це суттєво погіршить комунікацію у компанії. Також на певному рівні може бути доцільно заборонити працівникам використовувати свої власні пристрої, але знову ж це може призвести до тих самих незручностей; уявіть собі компанію з візуального дизайну, яка забороняє iPad. (Деякі правила, такі як заборона USB-накопичувачів, насправді можуть бути хорошим рішенням.)

Хоча “звичайні” інсайдери можуть стати зловмисними з різних причин, рідко ці причини походять з кіберпростору; натомість часто фізичний світ стає тригером. Тому важливо контролювати поведінку співробітників за межами кібердомену, щоб краще запобігти появі загроз.

Технології знижують бар’єр для зловмисної інсайдерської діяльності. Наприклад, крадіжка файлів на USB-накопичувачі менш злякає, ніж викрадення папок з картотеки, так само як розміщення облікових даних на веб-сайті простіше, ніж проникнення в заблокований кабінет. Наше сприйняття ризику також є трохи перекошеним у кіберпросторі, наша здатність логічно та раціонально міркувати серйозно обмежується в той момент, коли ми опиняємось перед екраном.

2.2 Соціальна інженерія

Соціальна інженерія - це мистецтво використовувати довіру когось і переконувати їх надавати свою конфіденційну інформацію. Він також відомий як злом людей, оскільки замість того, щоб націлювати машини, шахраї заманюють нічого не підозрюючих користувачів на викриття даних та розповсюдження шкідливих програм.

Шахрайство з соціальною інженерією розробляється на основі загальної поведінки людини. зловмисник розуміє, як створити паніку в свідомості жертви, або змушує його довіряти авторитетному голосу і робити все, що вони попросять.

Атаки соціальної інженерії мають два мотиви або цілі, і кожен зловмисник має намір досягти хоча б одного з них:

Саботаж: Порушення або пошкодження даних, щоб заподіяти незручності.

Крадіжка: крадіжка інформації або грошей.

Злом соціальної інженерії може траплятися за різними сценаріями. Це може статися на індивідуальному або організаційному рівні:

Індивідуальна соціальна інженерія

Хакер зв’язується з людиною за допомогою електронної пошти, тексту чи дзвінка. У повідомленні часто використовуються такі ключові слова, як "терміново", "безкоштовно", "останній шанс", "оновити платіжні реквізити", "термін дії пропозиції закінчується" тощо. Рядок теми та тон повідомлення виглядають і звучать правдоподібно. Щороку тисячі людей втрачають свої важко зароблені гроші через такі шахрайства.

Організаційна соціальна інженерія

Цей стиль соціальної інженерії подібний до того, що відбувається, коли на людину націлюють, але тут намір інший. Зловмисник надсилає зловмисну інформацію особі, сподіваючись, що вона поділиться своєю життєво важливою інформацією, надаючи хакеру доступ до даних, файлів та інформації про клієнтів своєї компанії. Зловмисник позначається як вищий орган компанії або хтось із IT-команди і вимагає ідентифікатор та пароль. Якщо стратегія успішна, вони потрапляють в організаційну систему, що спричиняє порушення внутрішніх операцій або крадіжку даних, грошей або інформації про користувача.

Як протистояти соціальної інженерії

Оскільки більшість із нас відкриває для себе радість Інтернет-світу, зло цієї системи також розкривається. Інформація та обізнаність дуже важливі, щоб уникнути нападу соціальної інженерії. Сформулюємо рекомендації що допоможуть зрозуміти, що таке соціальна інженерія та як не стати її жертвою:

Подумайте спочатку, дійте пізніше - соціальна інженерія створює відчуття терміновості, використовуючи тактику розмови під високим тиском. Завжди аналізуйте повідомлення та підтверджуйте, чи справді відправник.

Перш за все слід досліджувати посилання – багато посилань створені таким чином, що вони звучать як справжнє джерело, але в них відсутнє слово або помилка. "Я" замінено на "л", "О" стає "0", і так далі, і навпаки. Наведення курсора на посилання в електронній пошті покаже фактичну URL-адресу внизу.

Потрібно досліджувати факти - якщо ви ніколи не грали в лотерею, тоді немає шансів, що ви щось виграли. Аналізуючи контекст електронного листа, ви уникнете попадання в пастку зловмисних акторів.

Не треба завантажувати з ненадійних джерел - безкоштовні фільми, музика, ігри та інші речі, які коштують вам грошей на ринку, зазвичай завантажують якусь шкідливу помилку у вашій системі. Не завантажуйте все, що знайдете в Інтернеті.

Атаки через соціальну інженерію стануть головною проблемою в епоху глобалізації. Найефективніший спосіб запобігти цим проблемам у організації - це навчання кінцевих користувачів та підвищення обізнаності щодо кібербезпеки. Поінформованість - це єдиний спосіб запобігти атаці соціальної інженерії, оскільки з часом методологія також буде розвиватися. Сертифікована етична хакерська сертифікація Ради ЄС навчає всім методам та інструментам, які хакери використовують для компрометації систем. Це дозволяє використовувати ті самі інструменти та техніки проти поганих хлопців, щоб захистити своїх клієнтів.

Існує ряд готових сценаріїв соціальної інженерії, знаючи, що ви можете спланувати низку заходів щодо захисту інформації від атак інсайдерів, що дозволить вам розробити систему організаційних заходів захисту інформації від атак інсайдерів для конкретної організації у майбутньому:

Сценарій з новим працівником. Наприклад, представляючи себе керівником сусіднього відділу, правопорушник може попросити жертву, яка все ще не знайома з правилами безпеки, виконати певні дії на його комп’ютері. Він може пояснити таке прохання, описуючи деякі проблеми, з якими стикався. А жертва, намагаючись бути корисним, буде виконувати операції на потрібному комп’ютері (наприклад, додати

нового користувача для віддаленого доступу або завантажити шкідливе програмне забезпечення), не усвідомлюючи, що вона робить.

Щоб запобігти нападу, компанія повинна заборонити виконувати вимоги незнайомців, крім випадків, офіційно дозволених менеджером. Вирішені ситуації включають: запити, зроблені відомою людиною, коли голос точно розпізнаний; коли особу запитувача було перевірено завдяки спеціальним процедурам перевірки, описаним у рекомендаціях щодо створення політики безпеки; коли дія дозволена начальником або тим, хто добре знає людину.

Сценарій, коли працівники не знають про цінність інформації. Невідомість рівня важливості може спровокувати витік конфіденційної або критичної для бізнесу інформації. До цього типу працівників належать реєстратори, секретарі, телефонні оператори, адміністративні помічники, охоронці та інші.

Щоб запобігти нападу, інформація в організації повинна бути засекречена, працівники повинні бути навчені розпізнавати клас інформації. Якщо класифікація не була надана, вся інформація повинна сприйматися працівниками як конфіденційна, якщо не вказано інше.

Працівники відділу кадрів мають інформацію про структуру організації та про можливість контактів з іншими працівниками організації. Ця інформація може бути цінною для інсайдера на першому етапі атаки: отримавши інформацію про співробітників або, що ще більш небезпечно, працівників певного типу, зловмисник може більш точно планувати свою атаку, збільшуючи тим самим ймовірність її здійснення .

Для запобігання нападу необхідно розробити окремий підрозділ політики безпеки для відділу кадрів, використовуючи рекомендації щодо створення політики безпеки. Часто, представляючи себе менеджером іншого відділення, інсайдер може попросити відкриту інформацію (про наявність товару, якого немає у його відділеннях чи щось інше) і розпочати дружню розмову з жертвою. Після встановлення ділової дружби зловмисник може використовувати безліч засобів для отримання інформації, яка вже його цікавить. Наприклад, робити вигляд, що у їх філіях всі комп’ютери не працюють, і просити жертву переглянути якусь

інформацію про клієнта чи компанію. Після цього поговоріть «як завжди» з іншими жертвами про інші речі, і вона може потім не пам’ятати цього прохання. Коли настає час нападу, жертва втрачає пильність і обережність.

Тому важливо пам’ятати, що техніка формування довіри є однією з найефективніших тактик. Співробітники повинні завжди бути готовими до думки про те, чи добре вони знають людину, з якою нещодавно спілкувалися. Справді, в деяких випадках вона може бути не такою, якою претендує.

Сценарій використання страху жертви перед владою. Зловмисник використовує страх жертви перед босом або керівником компанії для отримання конфіденційної інформації. Більшість співробітників бояться своїх начальників і готові робити все, що завгодно, щоб не дратувати верхівку. Інсайдери також вміло цим користуються.

Наприклад, інсайдер телефонує жертві і намагається з’ясувати, де знаходиться його звіт, який жертва мала надіслати давно. Також зловмисник каже, що роботу, де використовується цей звіт, потрібно подати завтра, і керівник буде дуже незадоволений, коли дізнається, що зловмисник нічого не зробив для жертви. Під таким тиском і страхом «великого начальника» жертва готова якось передавати звіти, щоб не випробувати свого гніву.

Отже, навчання повинно проводитись для працівників, що повинно включати курс навчання персоналу, щоб уникнути впливу влади у дружніх або ділових стосунках, але без шкоди для спілкування.

Сценарій з небезпечним паролем. Зловмисник пояснює політику безпеки жертві, видаючи себе працівником відділу безпеки. Наприклад, інсайдер відволікає жертву, пояснюючи відомі принципи безпеки в організації. В процесі розмови він починає тему пароля жертви і з’ясовує, що вона використовує в ньому лише літери, а також цифри або додаткові символи. Потерпілий, швидше за все, не використовує лише літери. А зловмисник може запитати її пароль і запропонувати, як його змінити - додати цифри або символи в кінці. Зловмисник також пропонує можливість змінити пароль, і жертва приймає його.

Тому перед тим, як новим працівникам дозволено отримати доступ до комп'ютерних систем, вони повинні пройти навчання з правил безпеки, особливо правил нерозголошення паролів. Кожен має доступ до комп'ютера, повинен розуміти, що навіть така проста процедура, як зміна пароля, може призвести до серйозних порушень у безпеці системи.

Сценарій із напрямком об'єкта на неправильну адресу. Часто люди не помічають, що адреса сайту, з якого їх переспрямовують, відрізняється від оригіналу, хоча і схожа. Наприклад, користувач інтернет-магазину "books.com" може подумати, що адреса "books-nauka.com" - це також веб-адреса цього магазину, але з безпечним та тематичним доступом. Фактично ця адреса зареєстрована зловмисником спеціально для отримання особистої інформації користувача. Інтерфейс повністю скопійований з оригінального сайту, а також сприяє тому, що користувач нічого не помічає.

Потерпілий отримує лист із пропозицією отримати бонуси (гроші або участь у роздачі) за відновлення його особистої інформації на сайті, який жертва постійно використовує (Інтернет-магазини, аукціони). Але посилання, додані в кінці листа, ведуть не на потрібний сайт, а на сайт із подібною адресою. Жертва переходить за посиланням, бачить знайомий інтерфейс (повністю скопійований з оригіналу) і заповнює особисту картку, яка бажає отримати подарунок. Таким чином, зловмисник може отримати практично будь-яку інформацію про жертву.

У пошуках бонусів люди втрачають охорону. Але не так складно перевірити адресу посилання, на яке вони намагаються направити. Особливо у тому випадку, коли необхідно ввести особисту інформацію. Користувач повинен перевірити, чи відповідає сайт, на якому він вводить особисту інформацію, всім заходам безпеки. Або ввімкнено шифрування переданої інформації, сертифікати дійсності не застаріли.

Таким чином, виходячи з розглянутих сценаріїв соціальної інженерії, керівництво конкретної компанії може розробити політику безпеки та реалізувати заходи захисту інформації не лише на рівні програмного та апаратного захисту.

Дійсно, при будь-якому, навіть найвищому рівні технічного захисту інформації організації, залишається людський фактор, який не контролюється спеціально автоматизованими системами та програмами захисту інформації. Тому такий напрямок, як, наприклад, соціальна інженерія, цілком здатний показати низку інструментів-сценаріїв роботи з людським фактором. У нашому випадку завдання інсайдера в організації досягти успіху.

2.3 Загальні напрямки запобігання інсайдерським загрозам

Слід стежити за проблемами поза робочим місцем, беручи до уваги сімейні та особисті проблеми, медичні проблеми, фінансові проблеми та публікації в соціальних мережах, які не відповідають нормам. Супервайзери, фахівці з персоналу та, зокрема, співробітники служби безпеки повинні звертати увагу на поступові зміни в побутовій та життєвій ситуації. Коли відмічається зміна, така поведінка переводить суб'єкта до категорії підвищеного ризику для додаткового моніторингу.

Не слід забувати: що стосується інсайдерів, це частіше повільний перехід до зловмисної поведінки, аніж раптове падіння у прірву. Фінансові проблеми особливо актуальні, оскільки вони очевидно впливають на ризик отримання працівником взятки або продажу інформації в Інтернеті - і, як правило, з’являються поступово. Однак те саме можна сказати щодо особистих питань, таких як розлучення, медичних питань, таких як хворий член сім'ї, або дисциплінарних питань на робочому місці, таких як поганий ставлення на роботі. Інсайдерські загрози мотивовані цілим рядом причин, але причини є більш помітними, ніж можна було б подумати.

Слід почати моніторинг ще в процесі найму. Кандидати на роботу з історією імпульсивної чи деструктивної поведінки повинні негайно викликати підозру під час процесу пошуку. Зокрема, коли мова йде про сферу інформаційних технологій, винні в неправомірних діях або неналежній поведінці цілком імовірно повторять таку поведінку. Потрібно приділити подібну увагу підрядникам, про яких може бути менше безпосередньо доступної інформації.

Також слідкуйте за проблемами працівників на робочому місці. Чи є задоволеними працівники? Вони сперечаються з колегами? Вони раптово не виконують роботу або відсутні терміни? Вони незрозумілим чином відсутні протягом тривалого періоду часу? Це лише деякі поведінкові попереджувальні знаки про те, що щось може бути не так.

Така ж ретельність стосується змін у статусі зайнятості. Пониження, переведення, відрахування та припинення виплат підвищують ризик інсайдерської діяльності даного працівника. Пам'ятайте, що інсайдера не обов'язково звільняти, щоб він представляв активну загрозу; простий натяк на звільнення, пониження в посаді або щось подібне може бути достатнім для того, щоб співробітник відреагував. Досить часто співробітники, які залишають компанію, вживають руйнівних заходів до останнього дня (тобто викрадають власні дані або комерційну таємницю).

Звичайно, говорити «контролювати інсайдерів» без чітких зворотних зв’язків та механізмів звітування безглуздо. Отже: чітко спілкуйтеся та послідовно виконуйте політику безпеки та засоби контролю. Навчіть працівників з питань кібербезпеки, приділяти пильну увагу тому, як ви формуєте відповідні проблеми. IT-співробітники будуть розуміти безпечну кібер-поведінку зовсім інакше, ніж команда маркетингу. Подібним чином розуміння працівниками важливості безпеки буде різним - перше, з технічної точки зору або з точки зору управління ризиками, а друге, з точки зору зв’язків з громадськістю, наведемо лише один приклад.

Поряд з цим, не слід зосереджуватись занадто сильно на ризиках, які створюють інсайдери. Хоча потрібно навчити працівників з цього питання, надмірне повторення цього факту лише посилить недовіру та підірве спроби культури безпеки. Натомість зверніть увагу на те, як працівники можуть боротися з цією загрозою; позитивно сформулюйте потребу в обізнаності та допомозі та активно залучайте їх до своєї кіберзахисту. Зрештою, часто один інсайдер помічає неправильну поведінку іншого.

Слід зробити протоколи звітності надійними, добре відомими та конфіденційними - і навіть враховувати економічну вигоду анонімного звітування.

У міру надходження звітів переконайтеся, що технічні протоколи та протоколи безпеки людини швидко вмикаються. Ретельно документуйте свої розслідування та збір доказів, приділяючи особливу увагу корпоративній політиці та відповідним статутам та положенням.

Повідомлення не повинні стосуватися лише конкретних випадків, наприклад, хтось користується чужим комп'ютером, коли він перебуває поза робочим столом. Працівники також повинні мати можливість повідомляти про незвичну поведінку в цілому. Також час від часу треба нагадувати працівникам: те, що вони можуть не вважати доречним, насправді може бути дуже важливим.

Інсайдерські загрози для сучасного підприємства є серйозним ризиком, однак їх часто не беруть до уваги. Урядові установи та компанії повинні поєднувати технічні та людські протоколи моніторингу з регулярними оцінками ризиків, орієнтованою на людину освітою в галузі безпеки та міцною культурою корпоративної безпеки, щоб ефективно боротися з цією загрозою. Що стосується кібербезпеки, то обов'язковою є ситуаційна обізнаність, управління змінами, постійна пильність та повна адаптованість.

Висновки до розділу 2

У другому розділі були розкриті питання протидії інсайдерським атакам, визначено що таке Управління внутрішніми загрозами , його складові. Досліджено людське та етичне питання стеження та моніторингу працівників. Визначено технічну складову протидії інсайдерським атакам та підсумовано загальні напрямки запобігання інсайдерській загрозі.

РОЗДІЛ 3
ПРАКТИЧНІ АСПЕКТИ ПРОТИДІЇ ІНСАЙДЕРСЬКИМ АТАКАМ

Загалом існує 4 найбільш популярних методи протидії інсайдерській загрозі:

- Моніторинг працівників
- Запобігання втраті даних (DLP)
- Аналітика поведінки користувачів та організацій
- Поінформованість про безпеку або тренінги з кібербезпеки для працівників

3.1 Моніторинг працівників

Моніторинг працівників – процес відслідковування комп'ютерної діяльності працівників через маркери їхньої поведінки, такі як:

- Використання програм або програмного забезпечення
- Діяльність у інтернеті
- Використання соціальних мереж
- Час входу та виходу з системи
- Активний час проти простою

Багато організацій вирішують застосувати рішення для моніторингу працівників, намагаючись зменшити інсайдерські загрози. Моніторинг співробітників надає організаціям видимість повсякденної діяльності інсайдерів. На основі цього служби безпеки намагаються виявити закономірності та відхилення, які можуть бути ознакою підозрілої активності користувачів. Якщо сталося порушення, моніторинг працівників може надати запис про діяльність, яка допоможе відстежити походження вразливості.

Сучасні технології моніторингу співробітників використовують нові технології, такі як геолокація, реєстрація натискань клавіш, знімки екрана, запис відео та навіть доступ до веб-камер, встановлених на віддалених ПК. Хмарні обчислення означають, що ви можете захопити терабайт таких даних, які

зберігаються в Інтернеті та прості для менеджерів. Що ще важливіше, ці дані не просто лежать у стані неактивності, вони можуть використовуватися через складні алгоритми для передбачення внутрішніх загроз, вимірювання індивідуальної та командної продуктивності, а також для відстеження різних етапів, що ведуть до будь-яких проблем або витоків даних.

Як тільки інкогніто-агент встановлений на машині (іноді прихований у списку запущених процесів під замаскованими іменами), найпотужніші інструменти контролю за працівниками діють як всевидюче око. Вони можуть бачити все - від того, які програми відкрив працівник, з ким вони спілкуються та що говорять. Він навіть може використовувати автоматизовану логіку, таку як активатори ключових слів та правила політики, щоб повідомити адміністратора, коли співробітники роблять те, що вони не повинні робити.

Завдяки вдосконаленій автоматизації програмне забезпечення тепер може встановлювати різні попередження та тригери для пошуку шаблонів та компіляції проступків співробітників у звіти, які згодом можуть бути використані для побудови дисциплінарних справ проти них. І хоча працівникам це точно не сподобається, багато сучасних інструментів можна встановити в стелс-режимі. Що означає, що вони встановлюються та працюють у фоновому режимі ПК користувачів.

Все починається з знімків екрана та налаштованих параметрів запису екрану співробітників. Залежно від інструменту моніторингу співробітників, адміністратори компанії можуть налаштовувати правила та параметри для створення знімків екрана через певні проміжки часу - або один раз на годину, кожні 15 хвилин або навіть кожні 10 секунд або менше. Деякі інструменти також підтримують знімки екрана в режимі реального часу або безперервний запис відео, де адміністратор може зареєструватися в прямому ефірі на машині працівника або витягнути запис із позначкою часу певного періоду часу. Деякі інструменти дозволяють відтворювати, призупиняти або завантажувати знімки екрана. Найголовніше, що збережені знімки екрана також містять метадані і можуть бути включені в інформаційну панель моніторингу, щоб бути витягнуті як підтверджуючі докази або додаткові дані для

будь-якої діяльності користувача або точки даних, яку адміністратор переглядає або досліджує.

Людський фактор

Завдання цих рішень для глибокого моніторингу головним чином полягає у завершенні людського процесу. Більшість співробітників будуть занепокоєні, коли цей тип програмного забезпечення буде встановлено або, що ще гірше, виявлено. А менеджерам залишається стільки годин, щоб проглянути сотні, а то й тисячі знімків екрану протягом робочого дня працівника. Відеозапис - це наступний рубіж, який вже пропонують подібні Teramind, StaffCop Enterprise та Controlio. Доступ до відео в прямому ефірі або записаного відео забезпечує найточніші криміналістичні докази та можливість швидкого пошуку, очищення та навіть використання технології OCR для отримання повної інформації про документи, записані за допомогою відео.

Окрім самих зображень, ці моніторингові платформи можуть мати дивовижний ступінь детальної видимості кожного додатка, файлу, повідомлення та навіть дзвінків масштабування, які з’являються на екрані працівника або в його системі. Використовуючи OCR, глибокий моніторинг може отримати набагато більше подробиць про те, як працівники використовують конкретні настільні чи веб-програми, а найбільш пронизливий інструмент моніторингу співробітників буде аналізувати повідомлення електронної пошти, чати, миттєві повідомлення (IM) та інші особисті або командні програми для спілкування. Вони контролюватимуть будь-які параметри або навіть конкретні ключові слова, встановлені адміністратором. Досконаліші рішення можуть навіть знаходити номери кредитних карток та фінансові записи за допомогою скріншотів та відео та надсилати відповідні сповіщення, викликані цими дуже конкретними деталями.

Це глибоке відстеження стосується також відстеження документів та сканування імен файлів. Програмне забезпечення часто захоплює вкладений документ або файл, щоб адміністратор міг їх переглянути. Отже, якщо керівники C-Suite підприємства хочуть знати, чи спілкуються співробітники внутрішньо в чаті про генерального директора компанії або технічного директора, вони можуть просто налаштувати автоматичні тригери ключових слів, щоб отримувати сповіщення

електронною поштою, або всі згадки згрупувати у звіт. Ви можете налаштувати правила, щоб заборонити співробітникам надсилати дані компанії за особистими каналами, завантажувати програму чи файл, що не затверджений IT, або навіть вставляти USB-накопичувачі у ПК компанії. Не всі платформи можуть піти настільки глибоко в автоматизацію, але ті, які можуть запускати сповіщення користувачів, щоб зупинити дію, або просто надсилати попередження або оновлювати журнал аудиту.

Все це говорить про більш фундаментальне запитання: чи інвестує ваш бізнес в інструмент контролю за працівниками насамперед для підвищення продуктивності та ефективності? Або ви справді хочете або потребуєте повного контролю над усім, що роблять співробітники за часом компанії, до детальної деталізації? І як використання одного з цих інструментів дає змогу порівняти з вашими працівниками почуття дискомфорту, оскільки їх часто відстежують у власних будинках?

Вам потрібно ретельно продумати потреби вашої організації та те, яку цінність ви хочете отримати від впровадження подібного рішення. Тоді ви повинні вибрати інструмент моніторингу не лише виходячи з того, що вони можуть зробити, але як вони будуть застосовані та наскільки помітні будуть ваші працівники в цьому процесі.

Наведемо та проведемо порівняльний аналіз найбільш популярних існуючих систем(продуктів) у сфері моніторингу працівників:

Teramind

Teramind пропонує значний набір технологій, включаючи глибоке попередження та автоматизацію, а також відеозйомку за допомогою перегляду та записів сеансів у прямому ефірі. Це може забезпечити більш точне відображення активності співробітників у реальному часі на їх ПК.

Незважаючи на те, що він може бути застосований до різних випадків використання, основні функції Teramind включають моніторинг працівників, відстеження часу, виявлення інсайдерських загроз, дотримання вимог, оптимізацію продуктивності та захист від крадіжки даних. Менші компанії, яким потрібна

частина цих функцій, можуть виявити, що ціни та складність Teramind виходять за їх межі асортименту. Більші компанії, що мають конкретні потреби у дотриманні вимог або мають більш суворі потреби в безпеці (тобто суворі вимоги щодо інтелектуальної власності), прийматимуть залізний пакет моніторингу Teramind. Однак, якщо ви шукаєте щось, що вдвічі стане рішенням для управління проектами, знайте, що Teramind не будувався з урахуванням цієї можливості.

Функція глибокого відстеження Teramind може захоплювати будь-яку діяльність користувача, починаючи від звичайних записів екрану, переглядів робочих станцій ПК, відстеження електронних листів і навіть сеансів масштабування завдяки застосуванню відеозаписів сеансів у реальному часі, які також можна застосовувати до дистанційного навчання та сценаріїв усунення несправностей. Різноманітні інновації та надійні можливості моніторингу заробляють Teramind як вибір редактора у цьому сегменті.

Плюси:

- Широкий набір інструментів відстеження;
- інтуїтивно зрозумілий інтерфейс та інформаційна панель;
- унікальний перегляд сеансу в прямому ефірі та відеозапис;
- відстеження натискання клавіші;
- універсальне розгортання в хмарі або в приміщеннях;
- дотримання конфіденційності та контроль доступу.

Мінуси:

- поглиблені функції моніторингу можуть бути складними,

Veriato Cerebral

Те, що Veriato Cerebral представляє до таблиці, - це детальні, точні та ефективні дані для використання у реагуванні на інциденти, моніторингу інсайдерів з високим ризиком та звітності про продуктивність. Церебральний можна розгорнути локально, у хмарі або через керованого постачальника послуг (MSP). Агенти Veriato Cerebral, створені як рішення для виявлення інсайдерських загроз, стежать за кожною кінцевою точкою, оглядаючи будь-які витоки або підозрілі закономірності поведінки користувачів. Інтегрований ШІ активно вишукує загрози

та аномалії та запускає попередження. Що ще важливіше, Veriato Cerebral може використовуватися для відстеження даних в організації та блокування їх зовнішнього обміну.

Рішення також може відстежувати файли та документи в різних місцях, включаючи ті, що зберігаються на зовнішніх дисках, надсилаються через особисті облікові записи електронної пошти, роздруковуються або завантажуються на невідомі сервери. Цей тип відстеження безпеки неминуче охоплює моніторинг працівників. Коли ми розглянули це останнє, двома окремими пропозиціями Veriato були Veriato 360 та Veriato Recon. Veriato 360 був рішенням для моніторингу із захопленням та відстеженням знімків екрана, тоді як Veriato Recon зосереджувався на аналізі поведінки. Обидва продукти працювали спільно, але з тих пір були інтегровані у форму Veriato Cerebral.

Плюси:

- неперевершена видимість діяльності співробітників та спілкування;
- корисна інформаційна панель оцінки ризику виявляє різні типи загроз;
- потужні попередження про виявлення внутрішніх загроз;
- вимірює та аналізує залучення працівників;
- тверда суміш моніторингу та аналітики в одному інтерфейсі

Мінуси:

- може стати дорогим для великих команд;
- масивні файли даних можуть займати місце;
- дистанційне та приховане встановлення є складним завданням.

ActivTrak

Це рішення "Програмне забезпечення як послуга" (SaaS) пропонується через Google Cloud Platform і, як таке, може використовувати багато власних можливостей Google щодо аналізу великих даних, штучного інтелекту (AI) та безпеки. Аналітичні аналітичні дані дозволяють менеджерам певною мірою робити швидкі коригування на основі даних про співробітників у реальному часі. Інформаційну панель ActivTrak є однією з найпростіших для розуміння, хоча розбір і визначення того, які

види діяльності є продуктивними чи невиробничими, можуть бути досить нудними, особливо для великих компаній.

ActivTrak оснащений елегантним та чуйним інтерфейсом. Він пропонує просту установку агента та детальні та точні звіти, орієнтовані на продуктивність, та попередження нарівні з тим, що ви отримаєте від інструменту бізнес-аналітики. Він складається з міцного ядра інструментів моніторингу та функцій, створених для контролю доступу до даних та конфіденційності користувачів. Через ці особливості підхід ActivTrak до моніторингу співробітників є менш суворим для співробітників. Хоча це просто проникливе та всебічне, як і більшість інших рішень, орієнтація на підвищення продуктивності - це те, що співробітники можуть легко відстати.

Плюси:

- швидкий та інтуїтивно зрозумілий користувальницький інтерфейс;
- проста установка агента;
- може визначати провідні програми та веб-сайти, які використовуються;
- відстежує продуктивність на рівні проекту;
- моніторингові статистичні дані можуть бути використані для вдосконалення тренінгу співробітників.

Мінуси:

- потрібна тонка настройка для визначення показників продуктивності користувачів та груп;
- немає OCR для пошуку ключових слів на скріншотах;
- не вистачає реєстрації натискань клавіш;
- віджети інформаційної панелі не можна налаштувати.

3.2 Запобігання втраті даних

Запобігання втраті даних (DLP) – це інструменти та процеси, призначені для того, щоб конфіденційні дані не втрачались, не викрадались та не використовувались зловмисниками.

Є три основні інструменти DLP:

Network DLP – забезпечує захист конфіденційних даних у мережі вашої організації. Мережевий DLP відстежує всі мережеві комунікації навколо таких дій, як протокол електронної пошти та передачі файлів (FTP), позначаючи і попереджаючи вас про будь-які підозрілі дії в мережі.

Endpoint DLP – відстежує пристрої, що служать в якості точок доступу, здатних отримувати доступ до ваших конфіденційних даних, таких як ноутбуки, USB-диски та зовнішні жорсткі диски. Агент, встановлений на пристрої кінцевої точки, запобігає витоку даних та забезпечує користувачам видимість діяльності кінцевої точки.

Storage DLP – дозволяє контролювати доступ до конфіденційних файлів, що зберігаються та діляться особами, які мають доступ до вашої мережі, включаючи локальні та хмарні мережі.

Рішення DLP можуть значно зменшити ризик втрати даних внаслідок випадкової поведінки співробітників та порушення бізнес-процесів, що є причиною переважної більшості випадків втрати даних. Завдяки DLP фахівці з безпеки можуть зупинити втрату даних у своїх мережах, запобігаючи дорогим подіям безпеки.

Network DLP - це технологія захисту мережевих комунікацій організації, включаючи електронну пошту, веб-програми та традиційні механізми передачі даних, такі як FTP. Компанії використовують мережеві рішення щодо запобігання втраті даних, щоб запобігти втраті конфіденційної інформації через мережу. Ці рішення дозволяють компаніям шифрувати дані та належним чином блокувати ризиковані інформаційні потоки, щоб контролювати та контролювати потік даних через свої мережі та виконувати нормативні вимоги.

Як правило, запобігання втраті даних мережі включає можливість:

Перевірки та контролю трафіку електронної пошти, веб-пошти, веб-додатків, HTTP / S, FTP / S та TCP / IP

Отримати контроль і видимість веб-пошти та FTP, включаючи сеанси з підтримкою SSL

Запобігати втраті конфіденційних даних через мережу незалежно від порту або протоколу

Перевіряти теми електронної пошти, повідомлення та вкладення на наявність конфіденційного вмісту

Застосувати моніторинг та блокування веб-додатків на основі політики

Шифрувати вміст електронної пошти для безпечного спілкування та дотримання нормативних вимог

Повідомте користувачів та адміністраторів, коли мережевий трафік порушує корпоративні правила захисту даних

Для виконання своїх ділових ролей багатьом працівникам, партнерам та підрядникам потрібен доступ до конфіденційних даних компанії. Ці користувачі створюють, маніпулюють та обмінюються даними з безпрецедентно високою швидкістю, а це означає, що дані рухаються і вимикаються з корпоративної мережі, корпоративних та персональних пристроїв та хмари. Якщо у вашій компанії працюють незалежні підрядники та фрілансери, вони працюють поза корпоративною мережею, що робить ваші дані ще більшими ризиками втрати або ненавмисного впливу.

З цих причин пом'якшення інсайдерських загроз залишається основним варіантом використання мережевих рішень щодо запобігання втраті даних. Видимість даних та засоби управління, що надаються цими рішеннями, забезпечують захист на основі політики, щоб гарантувати, що конфіденційні дані передаються або отримують доступ до уповноважених одержувачів.

Хоча це найпопулярніший варіант використання мережевого програмного забезпечення для запобігання втраті даних, виявлення інсайдерських загроз все ще може бути складним завданням. Як правило, інсайдерські загрози виявляються складніше, ніж зовнішні атаки. Співробітники мають авторизовані логіни, тому їх спроби отримати доступ до даних не будуть розпізнаватися як загрози так легко, як спроби сторонніх осіб. З тієї ж причини інсайдерські загрози часто завдають більше шкоди, ніж зовнішні атаки. Деякі інсайдери також знають, яких заходів безпеки їм слід уникати, щоб не виявляти їх, крім того, їм не доведеться турбуватися про брандмауери та інші заходи безпеки на основі мережі, коли вони працюють усередині мережі.

Network DLP мають одну мету: зупинити конфіденційні дані від виходу з вашої організації. Є кілька ключових функцій, на які слід звернути увагу, вибираючи рішення щодо запобігання втраті даних у мережі, щоб ви мали впевненість, що ваші конфіденційні дані захищені. Надійне мережеве рішення щодо запобігання втраті даних повинно бути здатним:

- Автоматично попереджати або блокувати користувачів, коли діяльність визначається як ризикована на основі вмісту даних та контексту подій
- Автоматичне шифрування конфіденційних даних, які надсилаються електронною поштою або передаються на знімні пристрої або хмарні / веб-програми
- Ведення журналу подій для реагування на події та судово-медичного аналізу
- Забезпечення повноцінної перевірки вмісту з усвідомленням контексту для автоматичного розпізнавання конфіденційних даних, що потребують захисту
- Функції виявлення та класифікації даних для пошуку та позначення конфіденційних даних, щоб можна було застосовувати захисні політики

Наведемо та проведемо порівняльний аналіз найбільш популярних існуючих систем(продуктів) у сфері запобігання втраті даних:

SolarWinds Data Loss Prevention with ARM

Основні характеристики:

- Менеджер прав доступу
- Виявляє підозрілу активність
- Автоматизовані відповіді
- Аудит на відповідність стандартам захисту даних

Ключовою відправною точкою у вашій стратегії запобігання втраті даних є встановлення політики компанії щодо контролю доступу до даних. Менеджер прав доступу SolarWinds підтримує це завдання, надаючи чіткі звіти про поточні дозволи на доступ. Потім ви маєте можливість встановити кращі засоби управління, які можна впровадити через Менеджер прав доступу.

Поточний моніторинг постійно перевіряє доступ до даних та генерує попередження щоразу, коли копіюються або передаються дані. Менеджер уніфікує

моніторинг користувачів для Active Directory, Windows File Share, SharePoint та Microsoft Exchange. Це дозволяє контролювати діяльність користувача, який виявив незвичну або підозрілу поведінку в багатьох каналах зв'язку.

Плюси:

- Це надійне рішення для великих мереж, що підтримує як DLP, так і моніторинг дозволів для підтримки багатьох стандартів відповідності
- Добре інтегрується в існуючі середовища Active Directory
- Заощаджує час, створюючи прості візуалізації структур дозволів
- Використовує аналіз поведінки для виявлення інсайдерських загроз та порушень політики
- Може поєднуватися з автоматизацією, щоб заощадити час на відновлення та повністю уникнути відновлення даних

Мінуси:

- Високо детальне рішення, розроблене для системних адміністраторів у корпоративному середовищі - може зайняти час, щоб повністю вивчити та використати всі функції.

CoSoSys Endpoint Protector

CoSoSys пропонує Endpoint Protector як рішення на місці, як хмарну службу та як самостійний пакет програм. Місцева версія захистить комп’ютери під управлінням Windows, Mac OS та Linux. Центральний пристрій Endpoint Protector Server здійснює зв'язок по мережі з клієнтським програмним забезпеченням, встановленим на кожній кінцевій точці. Сервер також захистить підключені пристрої, такі як цифрові камери та USB-накопичувачі. Система Endpoint protector також доступна як програмне забезпечення, яке реалізує віртуальний пристрій на вашому власному сервері.

Основні характеристики:

- Платформа захисту кінцевих точок
- Пристрій, локальне програмне забезпечення або хмарна служба
- Відповідає стандартам HIPAA, PCI DSS та GDPR
- Також захищає приєднані пристрої

- Примусове шифрування

Повна система Endpoint Protector включає захист вмісту, контроль пристрою, примусове шифрування, виявлення мережі та управління мобільними пристроями. Доступна автономна версія для захисту лише однієї кінцевої точки за встановлення. Це Endpoint Protector Basic, і він включає модулі захисту вмісту та пристроїв у версії сервера.

Система захисту вмісту в Endpoint Protector керує передачею файлів відповідно до встановлених вами політик. Усі передачі файлів можна заблокувати для певних груп користувачів або дозволити переміщувати конфіденційні файли, якщо вони відповідають певним критеріям. Подібним чином, система керування пристроями може або повністю заблокувати приєднання пристроїв до захищеної кінцевої точки, або може дозволити передачу файлів за певних умов.

Плюси:

- Гнучка мультиплатформна опція для Windows, Linux та Mac
- Може відстежувати як окремі файли, так і окремі машини
- Попередньо налаштований для моніторингу відповідності HIPAA, PIC та GDPR
- Легко реалізувати власні набори правил

Symantec Data Loss Prevention

Рішення DLP від Symantec поєднує відстеження активності користувачів із контролем ризику даних. Він може контролювати дані, що зберігаються на серверах, робочих столах, мобільних пристроях та у хмарному сховищі. Початкова розгортка встановлення визначає всі місця, де зберігаються конфіденційні дані, і дає вам можливість видалити їх на центральний сервер управління, захистити сховище даних або закріпити на місці. Ви отримуєте шаблони та робочі процеси на відповідність стандартам HIPAA, GDPR та PCI DSS.

Основні характеристики:

- Відстеження активності користувачів
- Захист шифрування
- Відповідає стандартам HIPAA, GDPR та PCI DSS

Інструмент реєструє весь доступ до конфіденційних даних і відстежує ті облікові записи, які викликали попередження. Делікатні документи зашифровані і можуть бути переглянуті лише авторизованими користувачами. Інструмент також гарантує, що викинуті копії та вилучені документи повністю знищуються, не залишаючи в пам'яті жодних версій, які можна відновити. Усі копії відстежуються та зберігаються в безпеці, навіть коли вони розсилаються у віддалені місця або на мобільні пристрої, що належать користувачам.

Symantec DLP містить документи з конфіденційними даними за допомогою шифрування, і він визначає передбачуваних одержувачів шляхом відбитків пальців кожної копії. Це шифрування та ідентифікація доступу в парі з обмеженнями на переміщення даних та копіювання. Це дозволяє заблокувати приєднання файлів та даних до електронних листів або їх передачу через мережу чи Інтернет.

Система DLP Symantec є частиною системи захисту кінцевих точок. Тут здійснюється пошук вторгнень та зловмисного програмного забезпечення, яке може порушити конфіденційність ваших даних. Ця система включає моніторинг програмного забезпечення, яке не дозволено бізнесом, але встановлене на тому самому пристрої, що і конфіденційні дані - ситуація, яка особливо поширена у випадку використання користувацьких пристроїв для доступу до даних компанії.

Плюси:

- Поєднує DLP із відстеженням активності користувачів, надаючи йому додаткову функціональність
- Автоматичне сканування може нанести на карту делікатні місця, де зберігаються дані
- Пропонує заздалегідь побудовані храми та робочі потоки відповідно до основних стандартів відповідності, пропонуючи хороші функціональні можливості
- Підтримує моніторинг цілісності файлів через систему відбитків пальців

Мінуси:

- Могли б краще інтегруватися з іншими інструментами Symantec
- Потрібна краща функціональність для MacOS

3.3 Аналіз поведінки користувачів та організацій (АПКО).

User and Entity Behavior Analytics (UEBA) – це технологія виявлення кіберзагроз, заснована на аналізі поведінки користувачів, а також пристроїв, додатків та інших об'єктів в інформаційній системі.

Основною місією АПКО є своєчасне виявлення цілеспрямованих атак та інсайдерських загроз. Рішення АПКО обробляють велику кількість даних з різних джерел, визначають нормальні моделі поведінки для кожного користувача та об’єкта та повідомляють фахівців з інформаційної безпеки, якщо вони помічають відхилення від цих моделей.

Історія технологій АПКО

АПКО - це подальший розвиток технології АПК (аналіз поведінки користувачів). У 2014 році термін АПК(UBA) був введений у повсякденне життя аналітиками, тим самим позначивши нову категорію технологій захисту інформації, яку вони почали враховувати при складанні рейтингів постачальників, що виробляють програмне забезпечення для захисту інформації. Рішення АПК призначені для аналізу активності користувачів та ефективні у виявленні інсайдерських загроз та фінансових шахрайств (підозрілих операцій).

У 2015 році аналітики розширили відповідну категорію технологій безпеки, включивши аналіз поведінки "сутностей", тобто пристроїв, додатків тощо. Так з’явився термін АПКО. Основна різниця між АПКО та АПК зрозуміла з назви - якщо системи АПК аналізують лише поведінку користувачів, то системи АПКО також враховують поведінку "сутностей".

Як працюють системи АПКО

Рішення АПКО збирають та аналізують дані з різних джерел. Такі дані можуть включати:

- журнали серверів, робочих станцій, маршрутизаторів та інших пристроїв;
- реєстри систем контролю доступу та аутентифікації;
- дані інших рішень інформаційної безпеки - брандмауерів, антивірусів, продуктів SIEM та систем DLP;

- переписка користувачів у соціальних мережах, месенджерах, електронною поштою;
- реєстри персоналу компанії та інша інформація.

На основі зібраної інформації системи АПКО використовують машинне навчання та статистичний аналіз для формування моделей нормальної поведінки користувачів та сутностей. Згодом дані про діяльність користувачів та організацій узгоджуються з цими шаблонами. Якщо дія суттєво відрізняється від шаблону, наприклад, працівник надсилає листа топ-менеджеру, з яким він зазвичай не взаємодіє на роботі, або велика кількість даних передається на якийсь зовнішній сервер, система повідомляє фахівців із безпеки .

Продукти АПКО визначають закономірності в типовій поведінці користувачів, а потім виявляють аномальні дії, які не відповідають цим шаблонам і можуть спричинити проблеми безпеки. Крім того, системи АПКО виявляють нетипові події в різних об'єктах, які включають робочі станції, програмне забезпечення, мережевий трафік, системи зберігання даних тощо.

Для визначення відхилень, включаючи машинне навчання, використовуються різноманітні аналітичні методи. До речі, існує також клас систем АПК, які, як можна здогадатися, аналізують лише інформацію, пов’язану з користувачами та їх ролями. Джерелами даних для систем АПКО є файли журналів серверних та мережевих компонентів, системи безпеки, локальні журнали з ПК кінцевого використання.

Як правило, рішення АПКО виконують свою роботу після того, як інші кіберзахисту не вдалося виявити загрози в мережі.

Хоча рішення АПКО з’явилися нещодавно, вони швидко стали популярними у великих корпораціях. Крім того, багато постачальників включають функціональність АПКО в інші засоби захисту, такі як інформація про безпеку та управління подіями (SIEM), аналіз мережевого трафіку, управління ідентифікацією та доступом (IAM), захист кінцевих точок або запобігання. витоки даних. Аналітики Gartner прогнозують, що протягом п’яти років окремі продукти АПКО, які залишаться на ринку до того часу, перетворяться на рішення SIEM наступного

покоління, тоді як інші рішення АПКО знайдуть свою нішу в інших технологіях безпеки.

На наступному рисунку 3.1, можна побачити 3 основні стовпа згідно Gartner згідно яким система АПКО функціонує.

Рисунок 3.1 – Три стовпи АПКО згідно Gartner

Зокрема, згідно Gartner кожне рішення для АПКО повинно охоплювати кожен з таких критеріїв:

1. Сценарії використання:

- надавати уявлення про поведінку як користувачів, так і інших організацій;
- виконувати моніторинг, виявлення та попередження щодо аномальної поведінки як для користувачів, так і для суб’єктів;
- не зосереджуватись лише на одному випадку використання (наприклад, інструменти, що зосереджуються лише на спостереженні за працівниками чи довірених користувачів чи шахрайстві).

2. Аналітика:

- виявляти аномалії, використовуючи різноманітні підходи до аналітики - в першу чергу статистичні моделі та машинне навчання (machine learning, ML), але в поєднанні з правилами та підписами, поставляються як розфасована аналітика, яка використовується для створення та порівняння активності користувачів та організацій щодо їхніх профілів та профілів їхніх колег;
- розширені можливості аналітики, які не базуються на правилах, наприклад, використання алгоритмів кластеризації для динамічного групування однолітків;
- співвідносити діяльність та поведінку користувачів та інших суб'єктів та об'єднувати окремі ризиковані поведінки, щоб виділити аномальну активність.

3. Джерела даних:

- завантажувати дані про події від діяльності користувачів та сутності безпосередньо з джерел даних безпосередньо або через існуюче сховище. Рішення не повинні покладатися насамперед на мережеві дані як основне джерело даних і не повинні покладатися насамперед на власних агентів для збору даних телеметрії.
- збагачувати дані про користувачів контекстною інформацією та підтримувати потрапляння як структурованих даних подій у реальному часі, так і структурованих та неструктурованих довідкових даних з IT-каталогів (наприклад, Active Directory) або інших джерел інформації (наприклад, бази даних HR).

Наведемо та проведемо порівняльний аналіз найбільш популярних існуючих систем(продуктів) у сфері АПКО:

Exabeam Advanced Analytics

Exabeam пропонує рішення щодо безпеки та управління, які допомагають організаціям усіх розмірів захищати свою найціннішу інформацію. Продукти Exabeam використовують у своїй роботі технології машинного навчання та поведінкової аналітики.

На думку експертів Gartner, Exabeam Advanced Analytics є одним з найкращих у категорії АПК. Порівняно з конкурентами, це рішення дуже легко вивчити для системних адміністраторів або аналітиків, а це означає, що час його реалізації набагато коротший. Аналітикам не потрібно витрачати дні чи тижні на збір доказів

та складання інцидентів на основі інформації SIEM. Завдяки вдосконаленій аналітиці заздалегідь побудована шкала подій позначає аномалії та відображає деталі для повного захоплення події та її контексту.

Те, що раніше займало тижні, тепер можна зробити за лічені секунди. Інтерфейс користувача продукту зручний, навігація та перегляд історичних даних надзвичайно швидкі. Рішення містить сотні вбудованих моделей, деякі з яких унікальні і не можуть бути знайдені у конкурентів, що є головною перевагою продукту. Компанія пропонує кваліфіковану технічну підтримку своїх рішень.

На жаль, інструмент звітування практично відсутній. Користувач має можливість друкувати / експортувати вміст вікна браузера, надсилати попередження про ненормальні сеанси до системи SIEM, або він може просто робити знімки екрана. Якщо вам потрібно щось більше, вам потрібно вдатися до використання альтернативного інструменту. Для перегляду більше десятка подій у часовій шкалі потрібен монітор із високою роздільною здатністю, хоча навіть тоді не більше 20 подій помістяться. Існує спеціальна функція пошуку за допомогою панелі пошуку Threat Hunter, яка пропонує деякі досить хороші функціональні можливості.

Micro Focus Security ArcSight АПК

Аналіз поведінки користувачів ArcSight надає компаніям детальну інформацію про своїх користувачів, що значно полегшує створення даних про поведінку, щоб допомогти пом'якшити загрози. Це допомагає виявити та розслідувати зловмисну поведінку користувачів, внутрішні загрози та зловживання обліковим записом. Таким чином, це дозволяє організаціям виявляти порушення до того, як вони завдадуть значної шкоди.

ArcSight User Behaviour Analytics допомагає клієнтам зменшити ризик кібератак та виявити ненормальну поведінку, зіставляючи журнали системи управління ідентифікацією користувачів до інших IT-журналів, створених програмами та мережами. Крім того, продукт забезпечує швидшу реакцію на виявлені загрози завдяки глибокій інтеграції з SIEM, а також швидше розслідування інцидентів. Це пов’язано з тим, що АПК аналізує дані, пов’язані з користувачами,

визначає відхилення та порівнює їх із аналогами, історичною активністю та / або порушеннями заздалегідь визначеної очікуваної поведінки.

Таким чином, ArcSight АПК виявляє ненормальну поведінку користувачів, що дуже важливо для виявлення компрометації чи зловживання обліковим записом. Micro Focus пропонує найзріліші, перевірені випадки використання безпеки в АПК та симбіотичну безперебійну інтеграцію з SIEM.

Forcepoint АПКО

Аналіз поведінки користувачів та сутності Forcepoint (АПКО) дозволяє командам безпеки попереджувати моніторинг нестандартної поведінки високого ризику в організації. Аналітична платформа безпеки створює неперевершений контекст, поєднуючи структуровані та неструктуровані дані для виявлення та блокування зловмисних, скомпрометованих та недбалих користувачів. Forcepoint виявляє різноманітні критичні проблеми, такі як скомпрометовані рахунки, шпигунство підприємств, крадіжки інтелектуальної власності та шахрайство.

Оцінюючи нюанси взаємодії людей, даних, пристроїв та додатків, Forcepoint АПКО визначає пріоритети термінів для команд безпеки. Програмне рішення Forcepoint побудовано на чотирьох опорах:

Багатий контекст. Продукт об'єднує вміст, зібраний з різних джерел даних. Таким чином, доповнюючи можливості рішень SIEM та інших рішень у галузі інформаційної безпеки, виявляти та запобігати небажаним діям користувача.

Поведінкова аналітика. Forcepoint АПКО використовує кілька типів суворої поведінкової та контент-аналітики, орієнтованої на виявлення змін, закономірностей та аномалій з метою кращого виявлення складних атак.

Пошук і відкриття. Надає потужні засоби судово-медичного розслідування та виявлення через контекстний користувальницький інтерфейс для постійного моніторингу та поглиблених досліджень.

Інтуїтивно зрозумілий робочий процес. Забезпечує попереджувальну звітність, яка повністю інтегрується з робочим процесом системного адміністрування та існуючою архітектурою інформації про клієнта для оптимізації операційної ефективності.

Splunk User Behavior Analysis

Однією з головних сильних сторін аналізу поведінки користувачів Splunk є виявлення невідомих загроз та аномальної поведінки за допомогою машинного навчання.

Рішення Splunk User Behaviour Analysis пропонує наступні функції:

Розширене виявлення загроз. Продукт виявляє відхилення і невідомі загрози, які не беруть до виду традиційні інструменти безпеки.

Більш висока продуктивність. Автоматизує об'єднання сотень детектованих аномалій в єдину загрозу, що значно спрощує життя аналітика з безпеки

Потужні можливості розслідування інцидентів. Рішення використовує глибокі слідчі можливості і потужні базові характеристики поведінки для будь-якої сутності, аномалії або загрози.

Поліпшення видимості і виявлення. Автоматизує виявлення загроз за допомогою машинного навчання, що дозволяє приділяти більше часу усунення самих загроз і зміцненню безпеки.

Прискорена полювання за погрозами. Splunk User Behaviour Analysis швидко ідентифікує аномальні об'єкти без залучення людського участі. Рішення містить широкий набір різних типів аномалій (понад 65) і класифікацій загроз (більше 25) для користувачів, облікових записів, пристроїв і додатків.

Доповнені SOC ресурси. Автоматично об'єднує сотні аномалій, що спостерігаються в декількох сутності - користувачів, облікові записи, пристроях і додатках - в одну загальну загрозу для більш швидкої реакції.

3.2 Поінформованість про безпеку

Поінформованість про безпеку (Security Awareness) – це знання та ставлення членів організації щодо захисту фізичних, а особливо інформаційних активів організації. Багато організацій вимагають офіційного навчання обізнаності з питань безпеки для всіх працівників, коли вони приєднуються до організації та періодично після цього, як правило, щорічно.

Найбільш релевантні теми для тренінгів з питань кібербезпеки:

1. Фішинг

Фішингові атаки все ще є найпоширенішою причиною порушень кібербезпеки. Поточні цифри чітко відображають потребу в обізнаності про фішингові атаки, дослідження показують, що 91% успішних кібератак є результатом фішинг-шахрайства.

Незважаючи на те, що компанії дедалі більше усвідомлюють фішинг, у 2021 році це все ще зростаюча загроза, зокрема через відсутність обізнаності на рівні працівників. Проводячи навчання з безпеки як частину філософії компанії за допомогою періодичних тренінгів з підвищення рівня безпеки, ця кількість може значно зменшитися з часом.

"Spear Phishing" - це більш досконала і цілеспрямована форма атаки, що використовує конкретних працівників компанії для легітимації електронного листа до певного набору кінцевих користувачів.

Ось як це працює: приходить електронне повідомлення, мабуть, із надійного джерела, але натомість воно веде невідомого одержувача на підроблений веб-сайт, повний шкідливих програм.

Багато разів за цими нападами стоять профінансовані урядом хакери та хактивісти. Кіберзлочинці роблять те саме, маючи намір перепродати конфіденційні дані урядам та приватним компаніям. Ці зловмисники використовують індивідуально розроблені підходи та методи соціальної інженерії для ефективної персоналізації повідомлень та веб-сайтів. Як результат, навіть високопоставлені цілі в організаціях, такі як топ-менеджери, можуть виявити, що відкривають електронні листи, які вони вважали безпечними. Це проскакування дозволяє злочинцям викрадати дані, необхідні їм для нападу на їх мережі.

Навчивши своїх кінцевих користувачів розпізнавати потенційно шкідливі електронні листи та повідомляючи про підозрілі повідомлення, цю загрозу можна значно зменшити. Пропонуючи навчальні курси з кібербезпеки, поінформованість працівників про такі напади можна значно покращити шляхом послідовного

навчання. Імітовані фішингові атаки можуть продемонструвати потенційний ризик для вашої компанії від таких атак.

2. Знімні носій

Ще однією темою обізнаності щодо безпеки, яка щодня використовується компаніями, є знімні носії. Знімний носій - це портативний носій інформації, який дозволяє користувачам копіювати дані на пристрій, а потім видаляти їх з пристрою на інший і навпаки. Кінцеві користувачі можуть залишити USB-пристрої, що містять шкідливе програмне забезпечення, підключивши їх до свого пристрою.

Окрім розуміння ризиків, вашим працівникам потрібно знати, як безпечно та відповідально використовувати ці пристрої у вашому бізнесі. Існує безліч причин, за якими компанія вирішує використовувати знімні носії у своєму середовищі. Однак з усіма технологіями потенційні ризики завжди існуватимуть. Окрім самих пристроїв, важливо, щоб ваші співробітники захищали дані на цих пристроях. Незалежно від того, особисті вони чи корпоративні, всі дані мають певний вигляд.

Кілька найпоширеніших прикладів змінних носіїв, які ви та ваші співробітники можете використовувати на робочому місці:

- USB-накопичувачі
- SD-карти
- Смартфони

Цю тему щодо безпеки слід включити у навчання та охопити приклади змінних носіїв інформації, чому вони використовуються у бізнесі, а також те, як ваші співробітники можуть запобігти таким ризикам, як втрата чи викрадення знімних пристроїв, зараження шкідливим програмним забезпеченням та порушення авторських прав.

3. Паролі та автентифікація

Дуже простий, але часто проігнорований елемент, який може допомогти безпеці компанії – це захист паролем. Часто загальновживані паролі будуть підбиратися зловмисниками, сподіваючись отримати доступ до ваших облікових записів. Використання простих паролів або розпізнавання шаблонів паролів для працівників може спростити доступ злочинців до великого кола облікових записів.

Після крадіжки цієї інформації її можна опублікувати або продати з метою отримання прибутку в мережі Інтернет.

Впровадження рандомізованих паролів може значно ускладнити отримання зловмисними акторами доступу до ряду облікових записів. Інші етапи, такі як двофакторна автентифікація, забезпечують додаткові рівні захисту, які захищають цілісність облікового запису.

4. Фізична безпека

Якщо ви один з тих, хто залишає свої паролі на липких записках на своєму столі, можливо, ви захочете їх викинути. Хоча багато атак, можливо, відбуваються через цифрові носії, захист конфіденційних фізичних документів є життєво важливим для цілісності системи безпеки компанії.

Просте усвідомлення ризиків залишення документів, без нагляду комп'ютерів та паролів навколо офісних приміщень чи будинку може зменшити ризик безпеки. Застосовуючи політику «чистого робочого столу», можна значно зменшити загрозу викрадення або копіювання без нагляду документів.

5. Безпека мобільних пристроїв

Змінюваний ландшафт IT-технологій покращив здатність до гнучких робочих середовищ, а разом із цим і виникли нові можливості атаки на безпеку. Зараз у багатьох людей є можливість працювати в дорозі за допомогою мобільних пристроїв, це збільшення зв'язку пов'язане з ризиком порушення безпеки. Для невеликих компаній це може бути ефективним способом економії бюджету, однак підзвітність за користувальницькі пристрої стає все більш актуальним аспектом навчання в 2021 році, особливо для подорожуючих або віддалених робітників. Поява шкідливих мобільних додатків збільшило ризик використання мобільних телефонів, що містять шкідливе програмне забезпечення, що потенційно може призвести до порушення безпеки.

Онлайн-курси з найкращими практиками для працівників мобільних пристроїв можуть допомогти навчити співробітників уникати ризиків без використання дорогих протоколів безпеки. Мобільні пристрої повинні завжди мати захищену конфіденційну інформацію, зашифровану або з біометричною автентифікацією на

випадок втрати чи викрадення пристрою. Безпечне використання персональних пристроїв є необхідним навчанням для всіх працівників, які працюють на власних пристроях. Найкраща практика полягає в тому, щоб працівники повинні підписувати політику мобільної безпеки.

6. Віддалена робота

У 2021 році очевидна потреба у віддаленій роботі, у поєднанні зі збільшенням кількості користувачів, призвела до того, що багато компаній робили рішучі кроки до повного робочого дня, працюючи на дому. Віддалена робота може бути позитивною для компаній, а також розширення можливостей для працівників, що сприяє підвищенню продуктивності та кращому життю баланс. Однак ця тенденція створює підвищену загрозу для порушень безпеки, якщо вони не є безпечно освіченими щодо ризиків віддаленої роботи. Персональні пристрої, які використовуються в робочих цілях, повинні залишатися заблокованими, коли вони не перебувають без нагляду та мають встановлене антивірусне програмне забезпечення. Якщо компанія хоче запропонувати такий стимул, їм слід зосередитись на навчанні віддалених працівників безпечної практики праці.

Починаючи з 2021 року, цілком імовірно, що ця тенденція збережеться. Хоча ми сподіваємось, що офіси знову відкриються і повернуться до нормального трудового життя, компанії все частіше наймають віддалених працівників, і ті, хто адаптувався до способу життя при роботі з дому, можуть вважати за краще працювати таким чином. Очевидна потреба у навчанні працівників для розуміння та управління власною кібербезпекою.

7. Публічний Wi-Fi

Деякі співробітники, яким потрібно працювати віддалено, подорожувати в поїздах і працювати в дорозі, може знадобитися додаткове навчання з розуміння того, як безпечно користуватися державними послугами Wi-Fi. Фальшиві загальнодоступні мережі Wi-Fi, які часто видаються в кав'ярнях як безкоштовний Wi-Fi, можуть зробити кінцевих користувачів вразливими до введення інформації на незахищені загальнодоступні сервери.

Навчання користувачів безпечному використанню загальнодоступного Wi-Fi та загальних ознак для виявлення потенційної афери підвищить обізнаність компаній та мінімізує ризик.

8. Хмарна безпека

Хмарні обчислення спричинили революцію у бізнесі, способі зберігання даних та доступу до них. Ці цифрові програми перетворюють бізнес, однак, оскільки великі обсяги приватних даних зберігаються віддалено, виникає ризик масштабних злому. Багато великих компаній працюють над захистом даних, але, вибравши правильного постачальника хмарних послуг, хмарне сховище може стати набагато безпечнішим та економічно вигідним способом зберігання даних вашої компанії.

Хакерство з боку інсайдерів є набагато більшою загрозою, ніж для великих хмарних компаній. Gartner прогнозує, що до наступного року 99% усіх інцидентів у хмарній безпеці буде виною кінцевого користувача. Отже, навчання з питань кібербезпеки може допомогти працівникам забезпечити безпечне використання хмарних програм.

9. Соціальні медіа

Ми всі ділимося великими частинами свого життя в соціальних мережах: від свят до подій та роботи. Але надмірне розповсюдження може призвести до доступності конфіденційної інформації, що полегшить зловмисникам доступ до джерел зберігання даних.

Навчання працівників щодо захисту налаштувань конфіденційності їхніх акаунтів у соціальних мережах та запобігання розповсюдженню публічної інформації вашої компанії зменшить ризик потенційних можливостей, які хакери можуть отримати від такого доступу до вашої особистої мережі.

10. Використання Інтернету та електронної пошти

Деякі працівники, можливо, вже піддавалися порушенням даних, використовуючи прості або повторювані електронні листи для кількох облікових записів. Дослідження Hot for security показало, що 59% кінцевих користувачів використовують однаковий пароль для кожного облікового запису. Це означає, що якщо один обліковий запис скомпрометований, хакер може використовувати цей

пароль для робочих і соціальних мереж, щоб отримати доступ до всієї інформації користувача в цих облікових записах.

Часто веб-сайти пропонують безкоштовне програмне забезпечення, заражене шкідливим програмним забезпеченням, завантажені програми лише з надійних джерел є найкращим способом захистити ваш комп'ютер від встановлення будь-якого шкідливого програмного забезпечення. Навчання працівників безпечним звичкам в Інтернеті повинно бути ключовою частиною будь-якої індукції IT, хоча деякі можуть вважати цей тренінг очевидним, він є ключовою складовою безпеки будь-якої програми безпеки.

Багато великих веб-сайтів мали великі порушення даних протягом останніх років, якщо ваша інформація була внесена на ці веб-сайти, її можна було б опублікувати та викрити вашу приватну інформацію.

11. Соціальна інженерія

Соціальна інженерія - загальноприйнята техніка, яку зловмисники використовують для завоювання довіри співробітників, пропонуючи цінні приманки або видають себе за іншого співробітника для отримання доступу до цінної особистої інформації. Для боротьби з цими загрозами працівники повинні бути навчені темам обізнаності щодо безпеки, які охоплюють найпоширеніші техніки соціальної інженерії та психологію впливу.

Наприклад, представляючи себе життєздатним клієнтом або пропонуючи заохочення, приватна інформація може мимоволі передаватися цим зловмисникам. Підвищення обізнаності працівників про загрозу цих імітацій є критично важливим для зменшення ризику соціальної інженерії.

12. Безпека вдома

На жаль, загроза від злочинців не припиняється, коли ви залишаєте робоче місце. Багато компаній дозволяють своїм співробітникам використовувати їхні персональні пристрої, що є чудовим методом економії витрат і дозволяє гнучко працювати, проте з цим пов'язані ризики. Програми, завантажені зловмисним програмним забезпеченням на особисті пристрої, можуть загрожувати цілісності мережі компанії, якщо, наприклад, дані про вхід будуть порушені.

Крім того, зростаюча мережа цифрових ресурсів, доступних працівникам та компаніям, збільшила зв’язок та продуктивність. Однак ці додатки також становлять ризик для користувача, дослідження Propeller показало, що фішингові кампанії, націлені на dropbox, мали 13,6% кліків. Збільшення знань співробітників, обмін зашифрованими файлами та аутентифікація завантажень зменшать ризик.

Поряд з навчанням працівників темам підвищення рівня обізнаності щодо безпеки, у зв’язку із введенням нових нормативних актів, курс дотримання вимог стає все більш необхідним для працівників.

Співробітники також повинні знати про зміну фінансового регулювання, захисту даних, податків тощо. Зареєструвавшись на автоматизованих онлайн-платформах для управління політиками, ви можете постійно інформувати своїх співробітників про останні зміни в політиці та стежити за тим, щоб вони не забували про це.

Висновки до розділу 3

У третьому розділі роботи було проведено аналіз практичному аспекту методів протидії інсайдерським загрозам, таких як:

Моніторинг працівників – процес відстеження активності та діяльності працівників.

Data loss prevention – це інструменти та процеси, призначені для того, щоб конфіденційні дані не втрачались, не викрадались та не використовувались зловмисниками.

Аналіз поведінки користувачів та організацій – це технологія виявлення кіберзагроз, заснована на аналізі поведінки користувачів, а також пристроїв, додатків та інших об'єктів в інформаційній системі.

Security Awareness – це знання та ставлення членів організації щодо захисту фізичних, а особливо інформаційних активів організації.

А також запропоновано низку програмних рішень для для цих методів.

ВИСНОВКИ

Були проаналізовано наступні поняття:

Інформація з обмеженим доступом - це інформація, до якої має доступ тільки обмежена кількість осіб і розкриття якої заборонено відповідно до закону. Обмеження доступу до інформації здійснюється в інтересах національної безпеки або захисту законних прав фізичних та юридичних осіб.

Інсайдерська інформація - неоприлюднена інформація про емітента, його цінні папери та похідні (деривативи), що перебувають в обігу на фондовій біржі, або правочини щодо них, у разі якщо оприлюднення такої інформації може істотно вплинути на вартість цінних паперів та похідних (деривативів), та яка підлягає оприлюдненню відповідно до вимог, встановлених законом.

Інсайдерська торгівля - це торгівля акціями публічної компанії чи іншими цінними паперами (наприклад, облігаціями чи опціонами на акції) на основі суттєвої, непублічної інформації про компанію.

Інсайдер це:

- будь-яка особа (юридична або фізична), яка має доступ до конфіденційної інформації про діяльність фірми в силу свого службового становища або сімейних зв'язків;
- особа, яка в силу свого положення має доступ до важливої (фінансової) інформації, недоступною для широкого загалу. Операції з інсайдерськими акціями строго контролюються, реєструються і публікуються;
- особа, яка володіє більше 10% акцій товариства (підприємства, заводу і т. Д.).

Інсайдерську загрозу можна визначити коли поточний або колишній працівник, підрядник чи інший бізнес партнер, який має або мав санкціонований доступ до мережі, системи чи даних організації та навмисно неправомірне використання, що доступ до негативно впливає на конфіденційність, цілісність або доступність організації інформація або інформаційні системи.

Проведено аналіз частоти інсайдерських атак, кількості завданої шкоди, визначено які групи працівників становлять найбільшу загрозу для організації.

Досліджено основні напрямки протидії інсайдерським атакам, їхню моральну та етичну складову, та технічну сторону питання.

Проведено аналіз програмної частини протидії інсайдерській загрозі.

Data loss prevention – це інструменти та процеси, призначені для того, щоб конфіденційні дані не втрачались, не викрадались та не використовувались зловмисниками.

Аналіз поведінки користувачів та організацій – це технологія виявлення кіберзагроз, заснована на аналізі поведінки користувачів, а також пристроїв, додатків та інших об'єктів в інформаційній системі.

Security Awareness – це знання та ставлення членів організації щодо захисту фізичних, а особливо інформаційних активів організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України “Про доступ до публічної інформації” – ВВР, 2011, № 32, ст. 6 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/3480-15#Text

2. Закон України “Про цінні папери та фондовий ринок” – ВВР, 2006, № 31, ст. 268 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2939-17#Text

3. Закон України “Про інформацію” – ВВР, 1992, № 48, ст.21[Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

4. В.А. Савченко, В.В. Савченко, С.В. Довбешко – Нейромережева технологія виявлення інсайдерських загроз на основі аналізу журналів активності користувачів / Сучасний захист інформації – №4/2018

5. Cummings, Adam; Lewellen, Todd; McIntire, David; Moore, Andrew; Trzeciak, Randall (2012), Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector, Software Engineering Institute, Carnegie Mellon University,

6. Schoenherr, Jordan; Thommson; Robert (2020), Insider Threat Detection: A Solution in Search of a Problem, 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)

7. Coles-Kemp, Lizzie; Theoharidou, Marianthi (2010), Insider threat and information security management. In Insider threats in cyber security (с. 45-71).

8. Дудоров О.О., Каменський Д.В. – Інсайдерська інформація та кримінальний закон: від американських реалій до європейських перспектив – Юридичний науковий електронний журнал – № 3/2019

9. Анфіса Н.Н. – Поняття та ознаки інсайдерської інформації як особливого виду інформації з обмеженим доступом – Інформаційне Право – №4/2016

10. Що таке інсайдерська торгівля. Інсайдерська торгівля: хто такий інсайдер і чому його дії незаконні? Трейдинг на використанні загальної інформації [Електронний ресурс] - Режим доступу: https://promouvelka.ru/uk/chto-takoe-insaiderskaya-torgovlya-insaiderskaya-torgovlya-kto-takoi/

11. What Is Insider Information? [Електронний ресурс] - Режим доступу: https://www.investopedia.com/terms/i/insiderinformation.asp

12. INSIDER THREAT REPORT 2020, Cybersecurity insiders [Електронний ресурс] – Режим доступу: https://www.cybersecurity-insiders.com/wp-content/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pdf

13. І. П. Мігус, К. О. Голубенко, Розголошення інсайдерської інформації як загроза економічній безпеці акціонерних товариств – Економічна Наука – № 3/2012

14. Insider Threat Detection [Електронний ресурс] - Режим доступу: https://www.activtrak.com/insider-threat-detection/

15. SEI Insider Threat [Електронний ресурс] - Режим доступу: https://www.sei.cmu.edu/our-work/insider-threat/index.cfm

16. Combating the Insider Threat Guidance from NIST and the National Insider Threat Task Force [Електронний ресурс] - Режим доступу: https://www.tripwire.com/-/media/tripwiredotcom/files/white-paper/the_next_generations_perspective_on_combating_the_insider_threat_whitepaper.pdf?rev=63d6a733536a4234a50164d36bb6fe2f

17. Як спіймати інсайдера? [Електронний ресурс] - Режим доступу: https://www.mogroup.com.ua/?p=492

18. The CISO’s Guide to Managing Insider Threats [Електронний ресурс] - Режим доступу: https://securityintelligence.com/the-cisos-guide-to-managing-insider-threats/

19. DEFINITION of information governance [Електронний ресурс] - Режим доступу: https://searchcompliance.techtarget.com/definition/information-governance

20. FBI Insider Risk Evaluation and Audit [Електронний ресурс] - Режим доступу: https://web.archive.org/web/20121014005032/http://www.dhra.mil/perserec/reports/tr09-02.pdf

21. Combating the Insider Threat [Електронний ресурс] - Режим доступу: https://us-

cert.cisa.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf

22. Combating insider threats in the age of remote work [Електронний ресурс] - Режим доступу: https://www.securitymagazine.com/articles/94156-combating-insider-threats-in-the-age-of-remote-work

23. HowTo Combat the Insider Threat [Електронний ресурс] - Режим доступу: https://www.infosecurity-magazine.com/opinions/combat-insider-threat/

24. What is security awareness training? [Електронний ресурс] - Режим доступу: https://www.mimecast.com/content/what-is-security-awareness-training/

25. Insider threat management (ITM) [Електронний ресурс] - Режим доступу: https://www.g2.com/categories/insider-threat-management-itm

26. Top 15 Insider threat management Solutions for Enterprises [Електронний ресурс] - Режим доступу: https://pathlock.com/top-15-insider-threat-management-solutions-for-enterprises/

27. 10 Takeaways from Gartner 2020 Market Guide for Insider Risk Management Solutions [Електронний ресурс] - Режим доступу: https://www.code42.com/blog/10-takeaways-from-gartner-2020-market-guide-for-insider-risk-management-solutions/

28. How Does Insider Threat Detection Work & Why is it Crucial? [Електронний ресурс] - Режим доступу: https://www.logsign.com/blog/how-does-insider-threat-detection-work-why-is-it-crucial/

29. Market Guide for Insider Risk Management Solutions [Електронний ресурс] - Режим доступу: https://www.gartner.com/doc/reprints?id=1-251NZMFU&ct=210119&st=sb

30. Insider Threat: A Guide to Detect and Prevent Insider Threats [Електронний ресурс] - Режим доступу: https://www.lepide.com/blog/insider-threat-a-guide-to-detect-and-prevent-insider-threats/

31. What Is DLP and How Does It Work? [Електронний ресурс] - Режим доступу: https://www.mcafee.com/enterprise/en-us/security-awareness/data-protection/how-data-loss-prevention-dlp-technology-works.html

32. 5 Best Practices for Insider Threat Detection [Електронний ресурс] - Режим доступу: http://solidsystemsllc.com/insider-threat-detection/

33. What Is an Insider Threat? Understand the Problem and Discover 4 Defensive Strategies [Електронний ресурс] - Режим доступу: https://www.exabeam.com/UEBA/insider-threats/

34. How to Find Malicious Insiders: Tackling Insider Threats Using Behavioral Indicators [Електронний ресурс] - Режим доступу: https://www.exabeam.com/security-operations-center/how-to-find-malicious-insiders-tackling-insider-threats-using-behavioral-indicators/

35. Insider Threat Indicators: Finding the Enemy Within [Електронний ресурс] - Режим доступу: https://www.exabeam.com/UEBA/insider-threat-indicators/

36. Insider Threat Detection and Management [Електронний ресурс] - Режим доступу: https://www.securonix.com/solutions/insider-threat/

37. Top 10 Tips to Prevent Insider Threats[Електронний ресурс] - Режим доступу: https://securityboulevard.com/2020/09/top-10-tips-to-prevent-insider-threats/

38. Insider Threat Prevention Best Practices [Електронний ресурс] - Режим доступу: https://www.netwrix.com/Insider_Threat_Prevention_Best_Practices.html

39. INSIDER THREAT GUIDE [Електронний ресурс] - Режим доступу: https://www.dni.gov/files/NCSC/documents/nittf/NITTF-Insider-Threat-Guide-2017.pdf

40. Understanding Insider Threat Detection Tools [Електронний ресурс] - Режим доступу: https://www.exabeam.com/UEBA/insider-threat-detection-tools/

41. A DEFINITION OF NETWORK DATA LOSS PREVENTION [Електронний ресурс] - Режим доступу: https://digitalguardian.com/blog/what-network-data-loss-prevention

42. 4 Kinds of insider threats — and how to minimize them [Електронний ресурс] - Режим доступу: https://builtin.com/cybersecurity/insider-threat

43. Gartner Market Guide for User and Entity Behavior Analytics [Електронний ресурс] - Режим доступу: https://www.cbronline.com/wp-content/uploads/dlm_uploads/2018/07/gartner-market-guide-for-UEBA-2018-analyst-report.pdf

44. Как UEBA помогает повышать уровень кибербезопасности [Електронний ресурс] - Режим доступу: https://habr.com/ru/company/roi4cio/blog/436082/

45. How hackers are using COVID-19 to find new phishing victims [Електронний ресурс] - Режим доступу: https://www.securitymagazine.com/articles/92666-how-hackers-are-using-covid-19-to-find-new-phishing-victims

46. Режим доступу: Simple Steps to Protect Yourself on Public Wi-Fi [Електронний ресурс] - Режим доступу: https://www.wired.com/story/public-wifi-safety-tips/

47. 12 Essential Security Awareness Training Topics for 2021 [Електронний ресурс] - Режим доступу: https://blog.usecure.io/12-security-awareness-topics-you-need-to-know-in-2020

48. 59% of people use the same password everywhere, poll finds [Електронний ресурс] - Режим доступу: https://hotforsecurity.bitdefender.com/blog/59-of-people-use-the-same-password-everywhere-poll-finds-19851.html

49. What is social engineering and why is it important? [Електронний ресурс] - Режим доступу: https://blog.eccouncil.org/what-is-social-engineering-and-why-is-it-important/

50. 12 Best Data Loss Prevention Software Tools [Електронний ресурс] - Режим доступу: https://www.comparitech.com/data-privacy-management/data-loss-prevention-tools-software/

51. The Best Employee Monitoring Software for 2021 [Електронний ресурс] - Режим доступу: https://www.pcmag.com/picks/the-best-employee-monitoring-software

52. Небезпеки соціальної інженерії [Електронний ресурс] - Режим доступу: https://uk.aaa-apm.org/the-dangers-of-social-engineering-10160