МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

15.03 — КМР. 1939 –“С” 2022.12.30.014ПЗ

ПАВЛИЩЕ ОЛЕКСАНДРА МИРОСЛАВОВИЧА
2023 р.

НАЦІОНАЛЬНИЙ УНІВЕРСТИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

УДК 004.9-049.5

ЖЕНО»	**«ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ»**
Декан факультету інформаційних технологій	Завідувач кафедри комп'ютерних наук
Глазунова О.Г., д.п.н., професор	Голуб Б.Л., к.т.н., доцент
_____	_____
_____ 202_ р.	**«____ » _____ 202_ р.**

15.03 — КМР. 1939–"С" 2022.12.30.014 ПЗ

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему: Технологія управління інцидентами інформаційної безпеки з використанням DLP-систем

Спеціальність 121 Інженерія програмного забезпечення

(код і назва)

Освітня програма Програмне забезпечення інформаційних систем

(назва)

Орієнтація освітньої програми Освітньо-професійна

(освітньо-професійна або освітньо-наукова)

Гарант освітньої програми

Доцент,кандитат технічних наук _____ Голуб Б.Л

(науковий ступінь та вчене звання) (підпис) (ПІБ)

Керівник магістерської кваліфікаційної роботи

Доктор технічних наук, професор _____ Семко В.В.

(науковий ступінь та вчене звання) (підпис) (ПІБ)

Виконав _____ Павлище О.М.

(підпис) (ПІБ студента)

КИЇВ-2023

НАЦІОНАЛЬНИЙ УНІВЕРСТИТЕТ БІОРЕСУРСІВ

І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет (ННІ) **Інформаційних технологій**

ЗАТВЕРДЖУЮ

Завідувач кафедри комп'ютерних наук

Доц.,к.т.н. _____ Голуб Б.Л

(науковий ступінь, вчене звання) (підпис) (ПІБ)

«____» _____20_____року

З А В Д А Н Н Я

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ СТУДЕНТУ

Павлище Олександра Мирославовича

(прізвище, ім'я, по батькові)

Спеціальність 121 Інженерія програмного забезпечення

(код і назва)

Освітня програма Програмне забезпечення інформаційних систем

(назва)

Орієнтація освітньої програми Освітньо-професійна

(освітньо-професійна або освітньо-наукова)

Тема магістерської кваліфікаційної роботи: Технологія управління інцидентами інформаційної безпеки з використанням DLP-систем, затверджена наказом ректора НУБіП України від «30» грудня 2022р.

№1939 «С»

Термін подання завершеної роботи на кафедру 2023 11 05

(рік, місяць, число)

Вихідні дані до магістерської кваліфікаційної роботи: документ із навантаженням навчального плану на кафедру.

Перелік питань, що підлягають дослідженню:

1. Системний аналіз предметної області. Літературний огляд попередніх досліджень.
2. Моделювання методів дослідження.
3. Збір даних.

4

Аналіз даних. Результати.

Перелік графічного матеріалу (за потреби) допускається.

Дата видачі завдання «30» 12 2022 р.

Керівник магістерської кваліфікаційної роботи _____ Семко В.В

(підпис) (прізвище та ініціали)

Завдання прийняв до виконання _____ Павлище О.М.

(підпис) (прізвище та ініціали студента)

Анотація

У цьому дослідженні ми досліджували, які порушення Політики безпеки інформаційних систем (ISSP) можуть бути зменшені за допомогою впровадження рішень з запобігання витоку даних, які змушують дотримуватися ISSP для обмеження виходу даних за межі організації. Тому ми використовували концептуальний каркас, який поєднує теорію запланованої поведінки з навчанням та підвищенням обізнаності щодо безпеки (SETA), щоб визначити, чи витік даних є навмисним чи не навмисним на основі наміру особи та її дотримання ISSP.

У цьому дослідженні взяли участь дві організації, з якими ми провели інтерв'ю. Питання стосувались того, як вони вирішують ситуації витоку даних, як виглядає їхня Політика безпеки інформаційних систем (ISSP) та які дані вважаються конфіденційними. В обох організаціях була впроваджена система запобігання витоку даних (DLP), яка сканує і реєструє вихідні дані на основі ключових слів, які ми визначили на основі політик та загальної практики. їхній ISSP було також скопійовано та подальше проаналізовано разом із скануванням мережі та інтерв'ю, щоб отримати результат, який має відповісти на дослідницьке питання.

Результати наших виявлень показали, що в середньому відбувається більше ніж три випадки витоку даних щоденно. Здається, що всі вони були пов'язані з тим, що люди не дотримувалися процедур або політики. З іншого боку, не виглядає, що за цими випадками стояла зловмисна поведінка. Ще одним виявленням було те, що політики були не настільки добрими, як вони могли б бути.

Висновок цього дослідження полягає в тому, що навмисний витік даних може бути запобігнутий завдяки високому рівню культури безпеки та обізнаності щодо безпеки. Але ви не можете запобігти тому, про що не знаєте. Вам потрібна видимість щодо того, які дані покидають територію компанії, і система запобігання витоку даних (DLP) допоможе вам у цьому. Мати систему запобігання витоку даних буде технічною заміною високої культури безпеки, але це також може обмежити осіб з зловмисними намірами.

Abstract

gated by implementing data leakage prevention solutions which enforces the ISSP to limit what data that can leave the organization’s perimeter. We therefore utilized a

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

PII - Особисто ідентифікована інформація

ISSP - Політика безпеки інформаційних систем

IP - Інтелектуальна власність

TPB - Теорія запланованої поведінки

DLP - Запобігання витоку даних

HR - Відділ кадрів

PCI - Промисловість платіжних карт

AAA - Аутентифікація, авторизація, облік

DDoS - Розподілений запит на відмову в обслуговуванні

SETA - Навчання та підвищення обізнаності щодо безпеки

БД – База даних

ЗМІСТ

ВСТУП

Актуальність

За останні роки все більше організацій показують зростаючу обуреність витоками даних. Сучасні організації спираються на інформаційні системи для виробництва чи управління продукцією, яка є їхнім основним джерелом доходу. Це робить збереження даних в межах компанії надзвичайно важливим.

Середні витрати на витік даних досягли історичного максимуму у розмірі 4,35 мільйона доларів у 2022 році, згідно з новоопублікованим звітом про ціну витоку даних, що є зростанням на 2,6% порівняно з попереднім роком і на 12,7% з 2020 року.

Також нові дослідження показують, що 83% організацій, які брали участь у дослідженні, переживали більше одного випадку витоку даних, тоді як лише що брали участь у дослідженні, повідомили, що підвищили ціни на товари та послуги у відповідь на збитки, завдані внаслідок витоків даних.У 2007 році Велика Британія потерпіла витік даних у Відомстві доходів і митниць (HMRC), де внаслідок єдиного інциденту була скомпрометована особиста інформація 25 мільйонів людей. Отже, результати витоків даних не обмежуються лише економічними втратами.

Іншими поширеними наслідками витоків даних є втрата конкурентоспроможності та економічні витрати. Організації, які стають жертвами витоків даних, можуть опинитися в дуже складному становищі в боротьбі з іншими організаціями на тому ж ринку, оскільки їхні клієнти можуть вже не довіряти їм. Організація навіть може бути змушена виплатити компенсацію своїм клієнтам, чиї дані були компрометовані, що може бути надзвичайно важким для відновлення її репутації. Більшість організацій

витрачають кілька тисяч годин і значні кошти на розробку засобів безпеки та інших заходів для захисту свого майна, а також самої організації від загроз. Організації спираються на свою безпеку, щоб зберегти конфіденційні дані своїх клієнтів та своїх власних даних у безпеці від несанкціонованих осіб. Більшість організацій обурені можливістю втрати контролю над конфіденційними даними після того, як вони покинули межі організації. Як тільки конфіденційні дані покидають межі компанії, їхні основні переваги - конфіденційність, цілісність та доступність до них втрачаються.

Визначення проблеми

Раніше проведені дослідження показують, що більшість організацій зазвичай розробляють та впроваджують засоби безпеки, які передусім захищають їхні конфіденційні дані від зовнішніх загроз, але ігнорують внутрішні загрози. Це призводить до дисбалансу в архітектурі безпеки організації, де дані захищені від традиційних загроз, які намагаються прорватися через механізми безпеки ззовні організації. Здається, що ці механізми безпеки не заважають конфіденційним даним виноситися за межі організації, що є великою проблемою для більшості організацій.

Витік даних не обмежується вчиненням злочинних дій; він також може статися внаслідок нещасних випадків, і не рідко ненавмисний витік даних може бути більш серйозним, порівняно з умисним. Навіть якщо сам витік даних є негативним для організації, ненавмисний витік даних може завдати більшої шкоди організації, оскільки джерело витоку даних може залишитися невідомим і він може ставатися неодноразово.

Дослідження, проведене BERR, вказує на те, що більшість організацій не сканують свою вихідну комунікацію, не шифрують жорсткі диски та не запобігають виносу конфіденційних даних за межі організації. Це серйозна проблема, коли звичайний обмін електронною поштою з друзями може містити конфіденційні дані, що може призвести до витоку даних. За раніше проведеними

дослідженнями, більшість видів електронного спілкування не контролюється. Якщо конфіденційні дані надсилаються з організації через електронну пошту, то організація більше не може контролювати розголошення цих даних.

Сучасні організації намагаються заохочувати робочі практики через командну роботу і спільну відповідальність і покладаються на довіру та обмін інформацією. Організації бажають більш ефективного робочого місця, впроваджуючи командну роботу і спільну відповідальність, спираючись на довіру та обмін інформацією. Не рідко організації довіряють користувачам всередині меж організації, не надаючи суворої дисципліни, що породжує певні обурення стосовно витоку даних.

Мета дослідження та його завдання

Оскільки питання витоку даних стало значною проблемою для більшості організацій, метою нашого магістерського дослідження є аналіз того, як організації зіштовхуються з витоками даних, незважаючи на впроваджені правила (policies), спрямовані на вирішення проблеми витоку даних. Ця тема є дуже важливою для організацій та їхньої можливості запобігти виходу конфіденційних даних за межі організації. Це досягається шляхом проведення докладного кейс-дослідження політики інформаційної безпеки системи(ISSP) та витоків даних в організаціях.

Методи дослідження

Для збору інформації було проведено опитування працівників двох різних компаній.

Компанія 1 – державна компанія. У ній працює приблизно 800 працівників.. Вони надають послуги, характерні для муніципалітетів, такі як функціонування початкових шкіл, соціальні послуги і тд.

Компанія 2, яка брала участь у дослідженні, - це компанія з розробки програмного забезпечення з філіями в різних країнах Європи. Загалом у компанії працює

приблизно 400 співробітників, більшість з них працюють в Україні. Вони розробляють власне програмне забезпечення, яке продають своїм клієнтам. Крім того, вони надають віддалену підтримку своїм клієнтам за допомогою захищеного доступу до серверів на об'єктах клієнтів.

СИСТЕМНИЙ АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ. ЛІТЕРАТУРНИЙ ОГЛЯД ПОПЕРЕДНІХ ДОСЛІДЖЕНЬ

Для виявлення прогалин у дослідницькій галузі впровадження політики інформаційної безпеки системи (ISSP) і запобігання витокам даних нам необхідно ознайомитися з тим, що інші дослідники вже зробили до цього дослідження. Матеріали, доступні на обидві теми, є досить обширними, але під час нашого огляду літератури не виявлено впливу невпровадження політики ISSP.

Витік даних

Витік даних визначається як несанкціоноване розголошення конфіденційної інформації несанкціонованим особам через випадкові або навмисні дії (Shabtai's, 2012; Blasco, 2012; Annansingh, 2005). Bellinger (2004) стверджує, що дані є сирими і самі по собі не мають жодного значення. Якщо даним надаються значення через відношення до інших даних, вони змінюють свій стан на інформацію. Оглядаючи ці дослідження, можна зробити висновок, що дані впливають на інформацію та знання, і витік даних також може призвести до витоку інформації та знань. Виходячи з цього огляду, чи є витік даних фактично проблемою, оскільки дані визначаються як сирі і не мають значущості? Bellinger (2004) стверджує, що те, що хтось бачить як дані, інший може вважати інформацією. Якщо витікає величезна кількість даних, хтось може об'єднати їх у інформацію.

Colwill (2009) стверджує, що інсайдери існують в більшості підприємств, навіть якщо саме підприємство про них не знає. Це є причиною занепокоєння для багатьох компаній. Останнє дослідження RSA/IDC показало, що більшість головних інформаційних офіцерів (CSOs) більше турбуються про зовнішні загрози, і 82% респондентів навіть не знали, де знаходиться внутрішня загроза компанії. Дослідження також показало, що 5830 атак від зловмисників походили зсередини підприємства, і 5794 випадки, коли інсайдери зловживали своїми правами контролю доступу, і 19% атак були навмисними (Grant, 2009). Ponemon Institute щорічно публікує звіти про витік даних, і в 2013 році було зафіксовано

277 випадків витоку даних із середньою кількістю 23647 записів, які витекли. Середня вартість кожного запису становила 136 доларів (Ponemon Institute, 2013). Оглядаючи ці дослідження, можна визначити, що внутрішні загрози існують в межах підприємств прямо зараз, але керівництво з безпеки вибирає закривати на це очі, незважаючи на те, що одна атака компрометує кілька записів за високу ціну.

Інші дослідження кажуть, що 56% витоку інформації спричинене ненавмисними діями інсайдерів, тоді як 26% - навмисними.

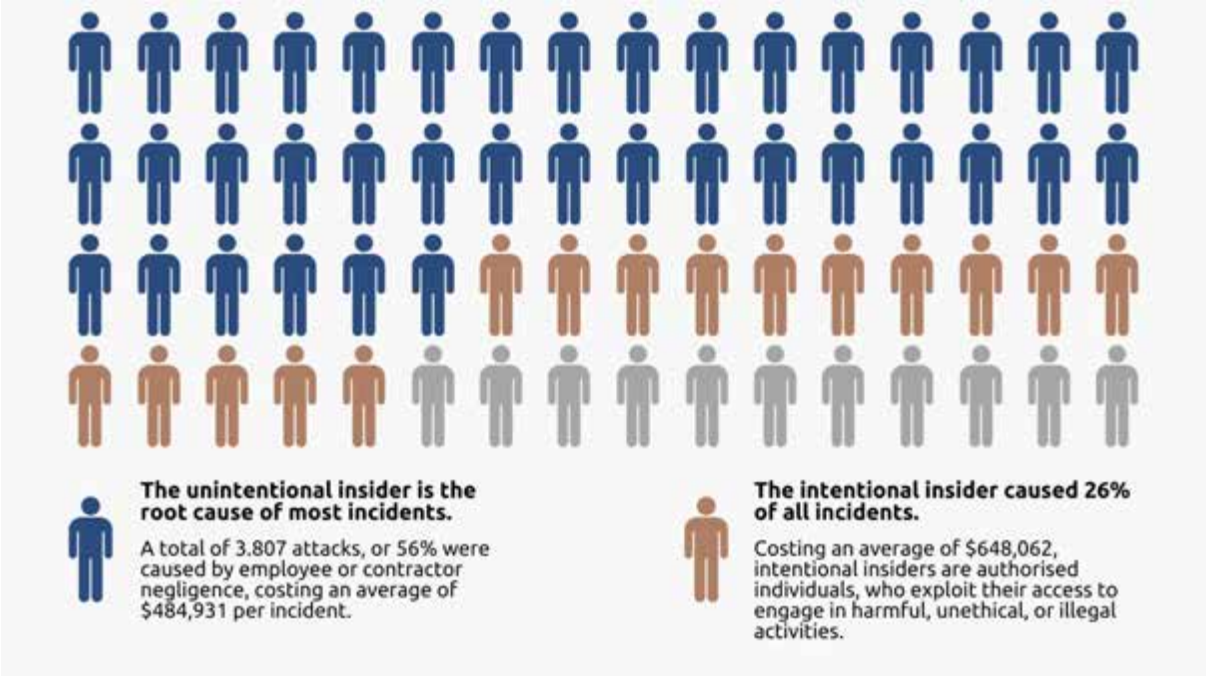

Рисунок 1Співвідношення інсайдерів

Дослідження BERR (2008) показує, що більшість організацій не перевіряє вихідну комунікацію на наявність конфіденційної інформації з метою запобігання витоку даних несанкціонованим особам. Електронна пошта, миттєві повідомлення, веб-пошта, форми на веб-сайтах, передача файлів та інші види електронної комунікації не контролюються і не підконтрольні після виходу з організації і можуть стати небезпечними, якщо конфіденційна інформація

потрапляє в неправильні руки (Blasco, 2012; Colwill, 2009). Інсайдер може відправити конфіденційні дані кому завгодно, оскільки відсутні заходи безпеки для запобігання виходу даних з підприємства, але є заходи для збереження даних поза ним. Якщо дані вийшли за межі підприємства, їх не можна зупинити від подальшого поширення, і вони можуть потрапити куди завгодно.

1.2 Запобігання витоку даних

Засіб для запобігання витоку даних (DLP) є технічним рішенням проти витоку даних, яке контролює і фільтрує вихідну комунікацію відповідно до конфіденційних даних (McCormick, 2008). Це підтверджується Blasco та Jorge (2013), які пояснюють, що рішення DLP працює, аналізуючи, моніторячи та контролюючи використання конфіденційних даних у системах обчислювальної техніки, щоб запобігти навмисному та випадковому витоку даних. ECS (2014) визначає моніторинг, аналіз і виконання наступним чином:

- Моніторинг(monitoring) належить до сканування мережевого трафіку в реальному часі, інспектуючи пакети даних на предмет конфіденційної інформації. Вони аналізують як вхідний, так і вихідний трафік, ідентифікуючи потенційні загрози, порушення політики або несанкціоновані передачі даних. Шляхом аналізу вмісту електронних листів, файлів, веб-запитів та інших каналів зв'язку DLP для мережі може застосовувати політику безпеки та запобігати витоку даних;
- Аналіз(analysis) належить до виявлення для ідентифікації конфіденційних даних в мережевому трафіку. Це може включати особисто ідентифіковану інформацію (PII), фінансові дані, інтелектуальну власність або конфіденційну бізнес-інформацію. Машинне навчання і алгоритми порівняння зразків часто використовуються для класифікації та маркування конфіденційних даних для подальшого аналізу та захисту;

- Виконання (enforcement) належать до будь-яких дій, які запобіжать витоку конфіденційної інформації. Це може бути блокування відправки файлів, блокування доступу до сесії і тд. Системи DLP для надають цінні відомості для реагування на інциденти та судових розслідувань. У разі подій із безпекою або витоку даних детальні журнали та сповіщення, які генерує рішення DLP для мережі, можуть допомогти визначити джерело порушення, уражені дані та події, які були вжиті. Ця інформація є важливою для зменшення впливу порушення та посилення заходів безпеки.

Деякі DLP створюють базу даних всіх відомих файлів в організації та сканують їх на ключові слова для позначення їх прапорцем. Якщо ці файли намагаються пройти повз корпоративний периметр, їх буде заблоковано. Інші рішення працюють, скануючи весь трафік, який проходить через брандмауер, і шукаючи ключові слова в реальному часі, використовуючи глибинну інспекцію пакетів, що навіть перевіряє вміст пакета. Схожою функцією у всіх цих DLP є можливість позначати документи на основі шаблонів. Якщо у вас є шаблон документа або презентації, де зазначено, що документ є конфіденційним, його не допустять до виходу за межі підприємства. Caputo (2009) та Lawton (2008) стверджують, що рішення DLP, які існують на ринку сьогодні, все ще мають багато проблем, проте певного прогресу досягнуто.

Призначення DLP - запобігти витоку конфіденційних даних з підприємства. Правильно налаштувавши DLP-систему компанії, можна усунути вихід певного типу інформації за межі компанії, або ж шифрувати вихідні дані за певним алгоритмом (ECS, 2014). Це означає, що рішення DLP може бути налаштоване для кожного окремого підприємства шляхом запобігання виходу даних, які вони визначають як нездатні покидати організацію. Нове покоління брандмауерів зазвичай мають функції, які працюють разом із рішенням DLP для запобігання несанкціонованому використанню даних, такі як Керування

додатками, яке блокує різні додатки та веб-застосунки на основі ідентифікатора додатка, а не порта сеансу TCP/UDP. Багато додатків працюють через TCP-порти H T T P або 443(HTTPS), і якщо блокувати ці порти, ви заблокуєте вхід та вихід до Інтернету.

1.3 Політика забезпечення безпеки інформаційних систем (ISSP)

Політика забезпечення безпеки інформаційних систем (ISSP) - це набір процедур, створених вищим керівництвом, щоб допомогти кінцевим користувачам дотримуватися стандартів безпеки, які необхідні для захисту знань компанії та збереження конкурентоспроможності. ISSP використовується для запобігання витоку даних і ґрунтується на довірі. Користувач читає, приймає та підписує ISSP, і якщо після цього не проводиться моніторинг чи здійснення ISSP, існує ризик витоку даних.

Існує багато причин, чому користувачі не дотримуються ISSP, але дослідження показують, що головна причина полягає в тому, що ISSP не відображає поточних практик. Отже, якщо організації не оновлюють свій ISSP, щоб відображати поточні практики та загрози, вони повинні вважати свою мережу та дані ненадійними. Другою причиною, яку виявив Lapke(2006), є опір вимогам безпеки.

Те саме дослідження також показує, що понад 50% користувачів в організаціях не знали поточного ISSP, і ще гірше було те, що більшість відділів безпеки організацій не знали про цю необізнаність. Якщо користувачі не знають ISSP, як можна очікувати, що вони будуть його дотримуватися? Якщо ISSP дотримується, організація не повинна проводити навчання при кожній зміні, інформування про здійснені зміни є достатнім.

1.4 Внутрішня загроза

Протягом останніх десятиліть підприємства витратили величезну кількість грошей і часу на розробку правил, політик, угод та інших засобів безпеки для забезпечення захисту своїх сховищ даних від загроз (Brendan, 2014). Недавнє дослідження показало, що 90% заходів безпеки організацій спрямовані на захист даних від зовнішніх загроз, тоді як 70% інцидентів сталися зсередини підприємства (McCue, 2008). Останні дослідження в галузі витоку даних показують, що організації все більше турбуються про витік даних, незаконне розголошення конфіденційних даних (Walker, 2008). Аналіз цих досліджень показує, що існує невідповідність між реалізацією заходів безпеки та реальними загрозами. Підприємства лише турбуються про внутрішні порушення безпеки, хоча вони відбуваються частіше порівняно з зовнішніми порушеннями безпеки, але вони зосереджуються на заходах безпеки проти зовнішніх загроз. У 2014 році в штаті Айова, США стався випадок. Два співробітники відділу соціальних служб Айови використовували онлайн сховище для зберігання робочого матеріалу, що не було дозволено згідно з ISSP. Відділу IT знадобилося 5 років, щоб помітити цей витік, і ніхто не знає, чи були дані, збережені в онлайн-сховищі, передані десь інде або використані протягом цих 5 років (Databreaches, 2014).

Зазвичай витік даних викликають «свої», які все більше стають ключовою проблемою для підприємств через їхню можливість розголошувати класифіковані дані незаконним сторонам. Внутрішні особи потенційно можуть завдати більшої шкоди організації, і для злоумисного користувача це має певні переваги порівняно з атаками ззовні. Вони мають привілейований доступ до даних підприємства, а також знання інфраструктури, вартості даних та способи приховування слідів втручання (Ahmad 2013). Проблема у тому, що такі люди вже мають легітимний доступ до конфіденційних даних через свою роботу. Це означає, що вони вже пройшли заходи безпеки, а тому можуть красти дані підприємства коли вважають це за потрібне. Знання про процедури підприємства дозволяє стерти сліди витоку даних та уникнути виявлення підприємством. У

події, яка сталася наприкінці 2014 року, працівник Memorial Hermann Health System мав доступ до медичних записів приблизно 10 600 пацієнтів протягом 7 років. Ці записи були доступні ПОЗА робочими годинами, і на даний момент ніхто не знає, для чого ці дані були використані, або чи вони покинули організацію (Roman, 2014). Кілька досліджень вказують на те, що витік даних може відбуватися внаслідок навмисних або випадкових дій внутрішніх осіб порівняно з навмисним. В опитуванні банківських і фінансових установ США 91% організацій, які брали участь в опитуванні, стверджували, що вони зазнали фінансових втрат, причому в 30% випадків збитки становили 500 000 доларів США і більше (Randazzo, 2005). Інше дослідження, проведене лабораторією Kaspersky, показує, що випадковий витік даних став більшою проблемою, ніж помилки програмного забезпечення. 27% компаній у цьому дослідженні втратили конфіденційні дані протягом останніх 12 місяців через ненавмисне розголошення інформації, і тільки 20% через вразливості програмного забезпечення (Kaspersky,

Оскільки більшість пристроїв в сучасному середовищі підключені до Інтернету, випадок витоку даних може призвести до незаконного розголошення конфіденційних даних перед усіма. Одного лише випадку витоку даних достатньо для завдання шкоди репутації та економіці підприємства. Простого клацання мишею вистачить для того, щоб інсайдер раптово завдав великої шкоди організації. Відбувалися випадки численних ненавмисних публікацій в Інтернеті. У Флориді в 2012 році підрядник відділу дітей і сім'ї, який займався перевіркою співробітників відділу, зберігав усі зібрані дані в Інтернеті без будь-якого виду шифрування. Вони були доступні для всіх, хто міг їх знайти, і ніхто насправді не знає, чи мав хтось доступ до цих даних.

1.5 Регулятивні вимоги та інтелектуальна власність

Відповідно до webspy (2009), існують два типи даних, які підприємства повинні захищати для запобігання витоку даних: дотримання регулятивних вимог та захист інтелектуальної власності.

- Дотримання регулятивних вимог: Кожне підприємство повинно дотримуватися певних місцевих та міжнародних регулятивних вимог, забезпечуючи, що конфіденційна інформація, особисто ідентифікована інформація і т. д. обробляються безпечно. Витік особистої інформації може мати серйозні наслідки, якщо несанкціоновані сторони отримають доступ до цих даних.

- Захист інтелектуальної власності: Захист важливих активів підприємства від тих, хто намагається вкрасти конфіденційні дані, та співробітників, які використовують такі дані для власних потреб, - це те, чого прагне досягнути запобігання витоку даних (DLP). Активи, які створили підприємства, такі як програми, формули і т. д., не призначені для виходу за межі підприємства, оскільки це може мати наслідки для самого підприємства. Якщо актив покидає межі підприємства, підприємство втрачає контроль над даними і їхнім використанням.

Підприємства більше не можуть ігнорувати проблему внутрішньої загрози, оскільки витік даних каже про недотримання регулятивних вимог, що суттєво впливає на бренд. Рішення щодо запобігання витоку даних повинні враховувати захист даних під час передачі, зберігання та використання. Кожна компанія є унікальною: чи вона виробляє щось, чи комбінує продукцію інших унікальним способом, надає послугу за спеціальну ціну, чи ще щось інше. Якщо секрет

бізнесу відкривається іншим, то будь-хто може відтворити таку ж компанію, а це є великим ризиком для першої. Останні дослідження показали, що випадки витоку даних, як правило, призводять до втрат репутації, конкурентоспроможності та економічних витрат. У 2007 році дані 25 мільйонів були розголошеними через внутрішню (insider) не системну помилку податкової служби Великої Британії (HMRC). Це дуже добре пояснює, чому інсайдери такі небезпечні і чому останнім часом підприємства стали більше перейматися витоком даних. Лише один випадок внутрішньої атаки може призвести до витоку величезної кількості конфіденційних даних, завдаючи шкоди репутації та економіці підприємства, а також втрати конфіденційної інформації про клієнтів. Ще один випадок стався в Південній Каролiні, США, де співробітник департаменту охорони здоров'я і соціального обслуговування отримав доступ до інформації щодо 228 000 осіб-клієнтів і нідслав ці дані на свою особисту адресу електронної пошти. Про їх подальше використання інформації немає.

Дослідження 12 різних порушень безпеки, які відбулися у 2006 році у великих американських компаніях, показують, що після порушення безпеки оголошення про цей випадок призвело до середнього зниження вартості компанії на 1% (Goel & Shawky, 2009). 1% може здатися незначним числом, але для компанії в мільярд доларів це вже досить багато. Це робить актуальним поновлення ISSP та виконання цих процедур. Інше дослідження свідчить про те, що виконання ISSP є інструментом, який суттєво покращує безпеку даних в організації (Knapp & Якщо ви виконуєте ISSP, ви автоматично маєте можливість проводити контроль, отримуєте звіт про те, хто де і як намагався вчинити дію, яка порушує поточний а отже матимете можливість прийняти міри для усунення подібних випадків.

Можливий наслідок невиконання комплаєнсу є важливим фактором для користувача(працівника) і значно впливає на його ставлення до дотримання усіх норм ISSP. Якщо він вважатиме, що незначне порушення не матиме негативних наслідків, то, будьте певні, він не буде вагатися перед порушенням правил і

положень. З іншого боку, якщо він знає, що його можна спіймати, і передбачено покарання за порушення правил, то, як показують дослідження, більшість користувачів буде дотримуватися правил. Але те ж саме дослідження показує, що, якщо є система винагороди для тих, хто дотримується правил, це буде важливим фактором для формування кращої культури безпеки в організації

O'Connor зазначає, що сучасні люди не можуть відмовитися від своїх електронних пристроїв, Інтернету тощо, оскільки це дозволяє їм працювати краще за короткий час. Хоча, багато компаній і намагаються обмежити доступ своїм працівникам до власних гаджетів, проте даний спосіб боротьби з витоком даних для деяких є не етичним. Сучасні люди є загрозою для конфіденційних даних через всі електронні пристрої.

Люди приєднують свій ноутбук до небезпечних мереж, підключають флеш-накопичувачі з вірусами, загалом пригоди, які можуть завдати значних збитків підприємству. Colwill (2008) стверджує, що шляхом шифрування конфіденційних даних можна уникнути виявлення, коли моніторинг DLP не має ключа для розшифрування.

Впровадження технічних рішень може допомогти зменшити витоки даних, але вони також можуть мати негативний вплив. Одним з аспектів є те, що помилкові позитиви (false positives) займуть час, і користувачі спробують обійти безпеку, якщо вона не працює так, як повинна, або використання її є не зручним. Опитування, що було проведене у 2006 році показує, що 34% всіх відповідачів стверджують, що заходи безпеки перешкоджають їх службовим обов'язкам (Post & Kagan, 2007). Це показує, що впровадження безпеки - це щось, що слід серйозніше сприймати усім – звичайним працівникам і керівництву компанії.

МОДЕЛЮВАННЯ МЕТОДІВ ДОСЛІДЖЕННЯ

2.1 Теорія запланованої поведінки

Теорія запланованої поведінки (TPB) - це передбачувальна теорія переконань, яку опублікував Айджен(також Айзен, Ajzen) у 1991 році, і вона є розширенням теорії обґрунтованої дії. Аджен стверджує, що TPB може передбачити наміри індивіда виконувати певні дії, аналізуючи ставлення індивіда до цих дій, суб'єктивні норми та сприйнятий контроль поведінки щодо цих дій. Теми, що становлять теорію запланованої поведінки, описані наступним чином за Ifinedo (2011):

Тема	Опис
Ставлення	ступінь почуттів індивіда щодо конкретної поведінки, в даному дослідженні - ставлення до виконання певних дій.
Суб'єктивні норми	сприйнятий соціальний тиск того, що люди навколо індивіда думають про цю поведінку, в даному дослідженні - вимоги щодо деяких дій.
Сприйнятий поведінковий контроль	визначається як сприйняття труднощів виконання певної поведінки. Уявний контроль поведінки є ключовою відмінністю між теорією запланованої поведінки та теорією зважених дій.

Табл. 1 Аспекти теорії запланованої поведінки

Рис. 2 Теорія запланованої поведінки

Теорія запланованої поведінки є однією з найбільш широко використовуваних передбачувальних теорій переконань і застосовується у різних областях досліджень. ТЗП також використовується в області інформаційної безпеки та політики забезпечення інформаційних систем (ПЗІС) і застосовується в численних дослідженнях, включаючи ті, які проводили Lee & Kozar, Venkatesh,

Декілька досліджень, що використовують теорію запланованої поведінки, прийшли до висновку, що ставлення, суб'єктивні норми та сприйнятий контроль поведінки впливають на наміри індивіда щодо виконання ISSP.

використали комбінацію кількох моделей у своєму дослідженні для розробки та емпіричної перевірки уніфікованої теорії прийняття та використання технології (UTAUT). У дослідженні були включені такі моделі, як теорія обґрунтованих дій (TRA), модель прийняття технології (TAM), модель мотивації (MM), теорія запланованої поведінки (TPB), поєднана TAM і TPB (C-TAM-TPB), модель використання ПК (MPCU), теорія поширення інновацій (IDT) та соціальна когнітивна теорія (SCT). Результатом було успішний інструмент, який може передбачати ймовірність того, що індивіди будуть дотримуватися правил.

Bulgurcu бажали ідентифікувати фактори, які впливають на те, щоб індивіди дотримувалися ISSP з метою захисту інформації та технічних ресурсів компаній. Теорія раціонального вибору була об'єднана з теорією запланованої поведінки. Результат дослідження показав, що ставлення, нормативні переконання та самоефективність впливають на наміри індивіда дотримуватися, і що ICA має позитивний вплив на ставлення індивіда та переконання у результаті.

Дослідження Lee & Kozar (2005) поєднало теорію запланованої поведінки з теорією поширення інновацій та інформаційну етику та мораль. Метою дослідження було з'ясувати, чому індивіди не використовують програми проти шпигунів, незважаючи на загрози, проведені шляхом емпіричного дослідження факторів, які впливають на рішення індивіда використовувати програмне забезпечення проти шпигунів. Висновок продемонстрував, що адаптація програмного забезпечення проти шпигунів впливає на ставлення, суб'єктивні норми, сприйнятий контроль поведінки та відмову від відповідальності. Інші фактори, такі як моральна обов'язковість, легкість використання впливали на наміри індивіда приймати менше, ніж вважалося.

з іншого боку, поєднали теорію запланованої поведінки з теорією обґрунтованих дій та моделями етичних рішень. Метою дослідження було розширити вивчення етичної поведінки в галузі IT, розробивши та перевіривши модель етичної поведінки. Результат показав, що ставлення та намір поведінки впливають на певні фактори, тоді як інші залежать від сценарію, і організації слід розглянути можливість впровадження навчань для запобігання небажаним зловживанням.

2.2 Поінформованість про безпеку

Обізнаність заходів безпеки є критичним аспектом програми управління інформаційною безпекою організації. Вона включає в себе навчання співробітників питанням безпеки (її найкращим практикам) і важливості

дотримання політики та вказівок щодо безпеки. Ось деякі ключові моменти, пов'язані із свідомістю щодо безпеки:

ипадковий та умисний витік даних: Дослідження показують, що витік даних може ставатися як умисно, так і випадково з боку внутрішніх працівників. Випадковий витік даних часто буває серйознішим, ніж умисний, оскільки його менше можна передбачити і він може бути наслідком недостатньої свідомості або розуміння політики щодо безпеки.
відомість кожного працівника про безпеку: Співробітники часто не мають достатньої свідомості по питаннях безпеки, які безпосередньо стосуються їх. Їх уявлення про загрози безпеці та її важливість можуть бути неточними і ґрунтуватися на особистому досвіді, або ЗМІ.
світа та навчання з питань безпеки: Багато дослідників і найкращі практики галузі підкреслюють користь програм освіти та навчання з питань безпеки. Програми з освіти, навчання та підвищення свідомості щодо безпеки безпекою. Ці програми допомагають користувачам зрозуміти політику безпеки, дізнатися про потенційні ризики та отримати необхідні знання для ефективного вирішення таких питань.

алучення користувачів: Ефективні програми свідомості щодо безпеки можуть залучати користувачів, роблячи їх більш зацікавленими та обізнаними у питаннях інформаційної безпеки. Ця збільшена свідомість спонукає користувачів дотримуватися правил безпеки, бути більш обережними та розуміти наслідки недотримання правил.
озуміння та прийняття вказівок: Кінцевою метою таких зусиль є забезпечення того, щоб індивіди розуміли вказівки та приймали необхідні міри щодо безпеки. Це розуміння сприяє культурі безпеки в організації, де співробітники серйозно ставляться до питань безпеки та мають мотивацію захищати конфіденційні дані.

Підсумовуючи, підвищення свідомості щодо безпеки за допомогою програм освіти, навчання та підвищення свідомості є важливим для зменшення ризику витоку даних та інших подій щодо безпеки в організації. Коли співробітники добре інформовані та розуміють важливість безпеки, вони більш схильні дотримуватися правил безпеки та допомагати захищати інформаційні ресурси організації.

.3 Концептуальна модель для дослідження

Для того, щоб дослідити, як витік даних може відбуватися незважаючи на наявність політики інформаційної безпеки та її впровадження, ми побудували нашу дослідницьку модель на теорії запланованої поведінки, щоб визначити, чи намір співробітника дотримуватися чи не дотримуватись такої політики є причиною витоку даних. Однак теорія запланованої поведінки не враховує ненавмисних витоків даних, що, як вказували попередні дослідження, можуть представляти рівносильну або навіть більшу загрозу, ніж навмисні витоки даних. У той час як теорія запланованої поведінки допомагає визначити, дотримується чи не дотримується індивід ISSP, все ще існує проблема ненавмисних витоків даних, яку попередні дослідження описували як відсутність обізнаності. Тому ми запропонували дослідницьку модель, побудовану на теорії запланованої поведінки як /причині навмисних витоків даних, поєднану з відсутністю свідомості, що призводить до ненавмисних витоків даних.

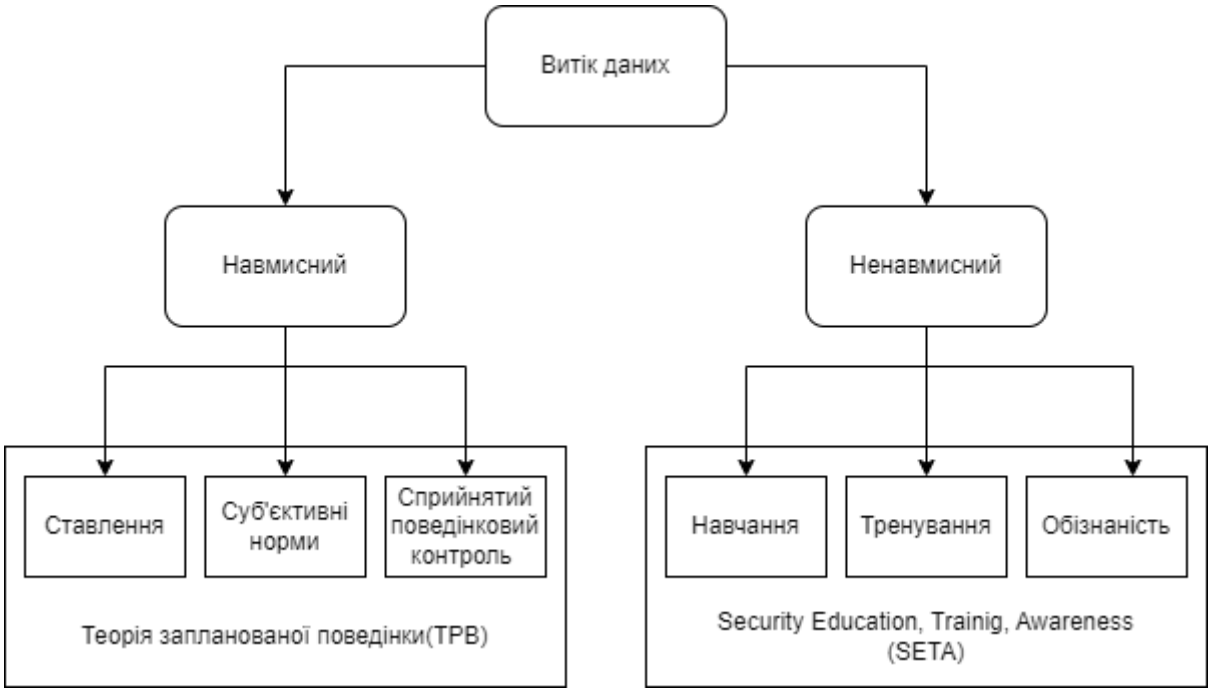

Рис. 3 Дослідницька модель

Суб’єктивні норми— це мотивація індивіда виконувати певну дію, на яку суттєво впливають спостереження або поради інших людей. Поведінка отучуючих керівників, співробітників або підлеглих), якщо ті показують ознаки виконання неабияк впливає на суб’єкта.

TPB вважає, що наміри поведінки є результатом ставлення цього індивіда до даного питання. Тому корисно як для організації, так і для індивіда, щоб останній мав позитивне ставлення. Щодо дотримання Політики інформаційної безпеки, особи з позитивним ставленням до неї більш ймовірно дотримуватимуться правил, вимог і вказівок. Це також діє у протилежному напрямку: особи з негативним ставленням, ймовірно, не будуть дотримуватися її.

Самоефективність передбачає здатність індивіда справлятися з певним завданням або приймати рішення, оцінюючи власну компетентність. Дослідження в галузі Політики інформаційної безпеки показали, що особи з більш високою компетентністю в галузі інформаційної безпеки будуть більш схильні дотримуватися ISSP порівняно з тими, у яких її менше. Очікується, що

особи з більш високою компетентністю в галузі інформаційної безпеки розуміють необхідність дотримуватися політики безпеки. Дослідження показали, що самоефективність є важливою та впливає на намір поведінки.

Освіта з питань безпеки призначена для того, показати кожному працівнику його роль та зону відповідальності стосовно ризиків і загроз інформаційної безпеки. Таким шляхом кожен учасник системи схильний уникати помилок.

Для того щоб оцінити ступінь обізнаності працівників, а також для «освіження пам’яті» потрібно проводити тренувальні навчання з питань безпеки Головна умова – проводити їх з певною частотою, адже люди схильні до забування інформації. Також, кожен день стається щось нове, а тому минулорічна інформація вже може бути застарілою. Метою навчання з питань безпеки є розвиток відповідних навичок та компетенцій з безпеки для підтримки робочої діяльності.

Метою підвищення свідомості щодо безпеки є переконатися, що особи усвідомлюють загрози та ризики, пов'язані з інформаційною безпекою. Це спрямовано на привернення уваги особи до питань безпеки та наслідків недотримання ISSP. Особи із вищою обізнаністю схильні до кращої практики безпеки, оскільки вони усвідомлюють ризики, свою відповідальність та як її виконувати.

Підхід до дослідження

Згідно з теорією Джона Крессвела існує три види дослідження: якісне, кількісне, змішане.

• Якісне дослідження є засобом для розуміння значеннь, яке індивіди або групи призначають соціальній або людській проблемі. Процес дослідження включає в себе постановку питання, збір даних, який зазвичай проводиться в присутності учасника, аналіз даних, котрий індуктивно розвивається від окремих (персональних) до загальних тем, з подальшою інтерпретацією значення даних дослідником. Заключний письмовий звіт має гнучку структуру. Ті, хто

займаються таким родом дослідження, підтримують підхід до дослідження, який враховує індуктивний стиль, акцент на індивідуальному значенні і важливість відтворення складності ситуації.

• Кількісне дослідження є засобом для тестування об'єктивних теорій, досліджуючи взаємозв'язок між змінними. Ці змінні, в свою чергу, можуть бути виміряні, зазвичай за допомогою інструментів, таким чином, що дані можуть бути проаналізованими за допомогою статистичних методів. Заключний письмовий звіт має фіксовану структуру, що включає вступ, літературу та теорію, методи, результати та обговорення. Так само, як і дослідники в якісних дослідженнях, ті, хто займаються цим видом досліджень, мають припущення щодо випробування теорій дедуктивно, включаючи заходи для запобігання упередженості, контролю за альтернативними поясненнями та здатності узагальнювати та реплікувати результати.

• Дослідження змішаним методом - це підхід до дослідження, який поєднує або асоціює як якісні, так і кількісні форми дослідження. Він включає філософські припущення, використання якісних і кількісних підходів і змішування обох підходів у дослідженні. Таким чином, це не просто збір і аналіз обох видів даних; це також включає використання обох підходів в одночасному режимі, щоб загальна сила дослідження була більшою, ніж у випадку якісних чи кількісних досліджень окремо.

У цьому дослідженні ми вирішили використовувати теорію запланованої поведінки (TPB) і SETA для визначення причин витоку даних, незважаючи на впровадження ISSP. TPB вже використовувалася в попередніх дослідженнях для визначення намірів індивідів дотримуватися ISSP, але, як показують інші дослідження, випадковий витік даних може виникнути, навіть якщо індивіди не

дотримуються ISSP. Тому наша теоретична база поєднує TPB і SETA для визначення, чи виникає випадковий витік даних через відсутність свідомості щодо безпеки, чи через навмисний витік даних, спричинений зловмисними особами.

Враховуючи вищенаведену інформацію стосовно різних методів дослідження, ми вирішили обрати якісний метод. Метою цього дослідження є зрозуміти поточний стан витоку даних в організаціях. Ми бажали поглибити наше розуміння цієї проблеми, досліджуючи дві різні компанії, які вразливі до витоку даних і як вони обробляють конфіденційну інформацію. Збір даних в цьому дослідженні базується на особистих інтерв'ю, документації та аналізі живого трафіку, щоб зрозуміти, як відбувається обробка конфіденційних даних. Оскільки метод збору даних є якісним, кількісний підхід до дослідження в цьому випадку не можна було б застосувати.

Ціль дослідження

Згідно з Baxter & Jack, мета дослідження використовується для пояснення загального характеру дослідження: чи опису випадку, чи його дослідження, чи порівняння між випадками. Yin описує цілі як пояснюючі, дослідницькі або описові.

- Пояснюючий підхід використовується, коли ви намагаєтеся пояснити припущені причинні зв'язки в реальних інтервенціях, які є занадто складними для опитувань чи експериментальних стратегій. Іншими словами, це служить для роз'яснення того, чому і як виникає зв'язок між змінними.
- Дослідницький підхід використовується, коли ситуація, яку ви оцінюєте, не має чіткого, єдиного набору результатів. Його можна використовувати для ідентифікації та отримання інформації, що надає інсайти щодо певної проблеми.

- Описовий підхід використовується для опису феноменів та реального життя, в якому вони виникають. Іншими словами, описова дослідницька ціль корисна для пояснення характеристик, які спостерігаються.

У цьому дослідженні ми досліджували, які види витоку даних існують в досліджуваних організаціях та як технічно відбувається витік. Ми хотіли переконатися, чи є потреба в зміцненні політики інформаційної безпеки, чи вона варта зусиль. Це вимагає відносно великих витрат і значної роботи для налагодження її якнайкраще, і нам потрібно особисто переглядати звіти про порушення, щоб переконатися, що те, що сталося, насправді є витоком даних.

Метою цього дослідження є вивчення того, як організації зіштовхуються з витоками даних, незважаючи на впровадження політики. Ідея полягає в тому, щоб зрозуміти, що таке витік даних, як він відбувається, і надати відомості про те, як ISSP може зарадити. Загалом, мета цього дослідження є дослідницькою.

Стратегія дослідження

Існують чотири різних стратегій дослідження, і кожна з них має свої власні переваги та недоліки:

ксперименти;

ослідження опитуванням;

наліз архівів;

a

s

e

-

s

t

u

d

y

. Кожна з цих стратегій може використовуватися для всіх трьох цілей дослідження: дослідницької, описової та пояснювальної. Отже, можливо вибрати будь-яку з цих чотирьох стратегій, оскільки це дослідження використовує дослідницький підхід. Проте у нашому випадку ні експерименти, ні дослідження опитуванням, ні аналіз архівів не підходять через вибраний нами метод збору даних.

Кейс-стаді є якісним підходом, який передбачає дослідження одного чи декількох кейсів. Кейси вивчаються докладно, і дані збираються з різних джерел інформації для створення опису та теми кейсу. Кейс-стаді - це стратегія дослідження, спосіб збору та аналізу даних. За Кресвеллом (Cresswell), існує три різновиди кейс-стаді: інструментальний, множинний(колективний) та інтринсичний кейс-стаді.

- Інтринсичні кейс-стаді спрямовані на вивчення незвичайного кейсу, який викликає особливий інтерес дослідника. Метою не є розробка теорії.
- Інструментальний кейс-стаді проводиться з метою надання уявлення про певну проблему, яка може бути загальнозастосовною. Отже, даний метод є індуктивним. Основною метою є сприяння поглибленому розумінню.
- Колективний кейс-стаді охоплює більше одного випадку з метою дослідження явища, популяції або загальної умови. Оскільки ціль - сприяти поглибленому розумінню, колективний кейс-стаді є об'єднанням декількох інструментальних. Використання підходу колективного кейс-стаді може відкрити можливість для більш глибокого тлумачення та "можливо кращої теоретизації".

Це дослідження фокусується на "як організації зазнають витоків даних, незважаючи на введені політики" і використовує кейс-стаді, проведений у трьох різних організаціях. Оскільки в трьох різних організаціях проводяться подібні кейси, це дослідження використовує стратегію множинного кейс-стаді, а не одиночного інструментального кейс-стаді. Шляхом виконання одного і того ж кейс-стаді в трьох різних організаціях ми можемо порівнювати патерни для отримання більш надійного результату.

.7 Метод збору даних

Однією з важливих особливостей кейс-стаді є використання різних джерел даних, що в свою чергу підвищує достовірність дослідження. Використовуючи кілька джерел, також можливо отримати краще розуміння проблеми порівняно з тим, що може надати одне джерело. Деякі джерела даних включають в себе

документацію, архівні записи, інтерв'ю, прямі спостереження та учасників спостереження. У цьому дослідженні ми вирішили використовувати документацію для вивчення політики інформаційної безпеки компанії, оскільки вона становить основу дослідження. Причиною цього є намагання дізнатись більш детально про організацію, про те яку інформацію вони вважають конфіденційною, як вони обробляють цю конфіденційну інформацію та як вони реагували на попередні порушення конфіденційної інформації, якщо такі були. Результати аналізу документації також надали нам базовий план того, яку інформацію шукати при виконанні аналізу трафіку. Наприклад, якщо політика вказувала, що та інформація, яку можна ідентифікувати стосовно якоїсь особи є конфіденційною, ми створювали фільтр, який шукав номери соціального страхування в інформації, яка залишає компанію. Під час аналізу ISSP ми також шукали докази будь-якого процесу SETA, щоб визначити, як вони проводили навчання для запобігання ненавмисному витоку даних відповідно до нашого теоретичного базису.

Пряме спостереження також було використано в цьому дослідженні, оскільки воно охоплює те, що фактично відбувається всередині організації. Для проведення прямого спостереження щодо витоку даних ми вибрали аналіз трафіку, розмістивши моніторинговий брандмауер паралельно з існуючим брандмауером організації. Цей паралельний брандмауер збирав всю інформацію, яка проходила через периметр компанії, і шукав ключові слова в даних, не заважаючи діяльності організації. Цей брандмауер був встановлений на дзеркальному порту існуючого брандмауера, тобто він не виконував активних дій на основі даних, а лише прослуховував та аналізував отримані дані. Він перевіряв дані пакетів і шукав попередньо визначені ключові слова, які базувалися на інтерв'ю та найкращих практиках. Наприклад, якщо ISSP вказує, що BitTorrent є незаконним згідно з політикою, така подія відстежувалася. Проте ми також хотіли дослідити, який тип даних був віправлений під час сесії BitTorrent. Чи була це конфіденційна інформація, чи просто хтось завантажував безкоштовний додаток

чи щось інше з Інтернету? На основі типу події ми робили припущення про подію, щоб категоризувати їх як навмисні чи ненавмисні, на підставі нашого теоретичного каркасу.

Ми також проводили інтерв'ю, спрямовані на існуючі заходи, які були прийняті компанією для обмеження витоку даних. Прикладами питань є: «чи є визначена роль, відповідальна за оновлення ISSP?», «як вони виконують оновлення?», «як користувачі повідомляються про внесені зміни?». Ми також намагалися дізнатись, чи відомо про які-небудь випадки витоку даних та як вони реагували або планували реагувати на такі події. Ми також намагалися визначити, які дані найважливіші для компанії, яку інформацію потрібно найбільше захищати та як вона захищена на сьогоднішній день. Основною метою інтерв'ю було краще познайомитися з компанією, відобразити типи даних в політиці інформаційної безпеки та в нашій стратегії збору даних, а також розкрити їх стратегію SETA. Стратегія SETA була важливою для нас, щоб отримати знання про обізнаність співробітників і слідувати нашому теоретичному каркасу.

.8 План аналізу

Метою аналізу даних є категоризація, табулювання або якимось іншим способом поєднання зібраних даних для відповіді на початкове питанян дослідження. У цій фазі зусилля спрямовано на оцінку даних, зібраних з попереднього етапу дослідження. Пропонується п'ять аналітичних технік, які можуть бути використані для аналізу зібраних даних: порівняння паттернів, побудова пояснення, аналіз часових рядів, логічна модель та синтез між кейсами.

Порівняння паттернів є однією з найбільш бажаних технік аналізу, яка включає в себе порівняння емпірично-базованого паттерну з передбаченим паттерном. Кейс-стаді може набути достовірність, якщо паттерни взаємно відповідають один одному, але паттерни також можуть бути релевантними, навіть

якщо вони не відповідають один одному. Порівняння паттернів корисне для виявлення простих паттернів та для переконання, що ті результати, що показали попередні дослідження - коректні. Також така техніка корисна для виявлення конфліктів, які не відповідають паттернам.

Синтез між кейсами спеціально розроблений для досліджень з використанням кількох кейсів і є найкращим вибором, коли є два чи більше кейси. Аналіз та результати ймовірно будуть простішими та надійнішими, ніж при одиночному кейс-стаді. Попередні чотири техніки не підходять нам, адже вони обмежені одиночними кейс-дослідженнями. Аналіз більшої кількості кейсів може дати більш надійний результат.

Інтерв'ю були подібні для всіх компаній, і вони включали основний набір запитань, які задавалися під час всіх інтерв'ю. Відповіді записувалися та погоджувалися з респондентами перед їх використанням у дослідженні. Відповіді порівнювалися з існуючою політикою інформаційної безпеки за допомогою порівняння паттернів. Оскільки всі компанії в дослідженні повинні бути порівнюваними і мати однаковий погляд на безпеку, ми також порівнювали відповіді різних компаній стосовно політики інформаційної безпеки за допомогою порівняння паттернів для виявлення відмінностей у поглядах на важливість даних та способи їх захисту навіть серед схожих компаній.

Аналіз трафіку проводився з використанням брандмауера зі загальною системою захисту від загроз та захисту від витоку даних. Однією з важливих рис цього брандмауера є можливість генерації подій журналу на основі різних тригерів, які ми визначаємо. Ми визначили правила, які активувались на події, які не відповідали політиці інформаційної безпеки або де пакети складалися з важливих даних, які не повинні витікати. Наприклад, якщо компанія вважає, що вихідний код є конфіденційним і він не повинен залишати територію компанії, ми створювали тригер, який шукав такий код в даних, які залишають периметр, а далі створював подію на основі цього. Ми використовували інструмент, який може генерувати звіт на основі зареєстрованих подій, і цей звіт використовувався

як вхід для нашого аналізу трафіку. Більшість сучасних брандмауерів наступного покоління можуть створювати такий звіт, але можуть бути і помилкові позитиви і дані, які потрібно пояснити. Ми використовували звіт як початкову точку для докладного дослідження подій, які були цікаві для дослідження, використовуючи техніку побудови пояснень. Наприклад, якщо подія була зареєстрована щодо витоку вихідного коду, ми докладніше розглядали цю подію. Можливо, це просто користувач поставив загальне питання на форумі, додаючи трохи загального коду, щоб вирішити завдання.

Теорія запланованої поведінки передбачає, що намір особи дотримуватися ISSP визначається трьома факторами, однак вона не застосовується до ненавмисного витоку даних. Тому ми вважаємо, що ненавмисний витік даних спричиняється іншими факторами, які можуть бути покриті SETA. На підставі нашої концептуальної моделі, шляхом перехресного аналізу даних, зібраних в організаціях, можна визначити, чи є витоки даних навмисними чи ненавмисними.

ЗБІР ДАНИХ

3.1 Огляд використаних інструментів

Для проведення аналізу трафіку ми використовували брандмауер Checkpoint, який був встановлений у режимі "tap" на дзеркальному порту комутатора, до якого підключено зовнішній інтерфейс існуючого брандмауера компанії. Таким чином, ми подавали встановленому брандмауеру Checkpoint ті ж дані, що і існуючий брандмауер, як в напрямку виходу, так і в напрямку входу.

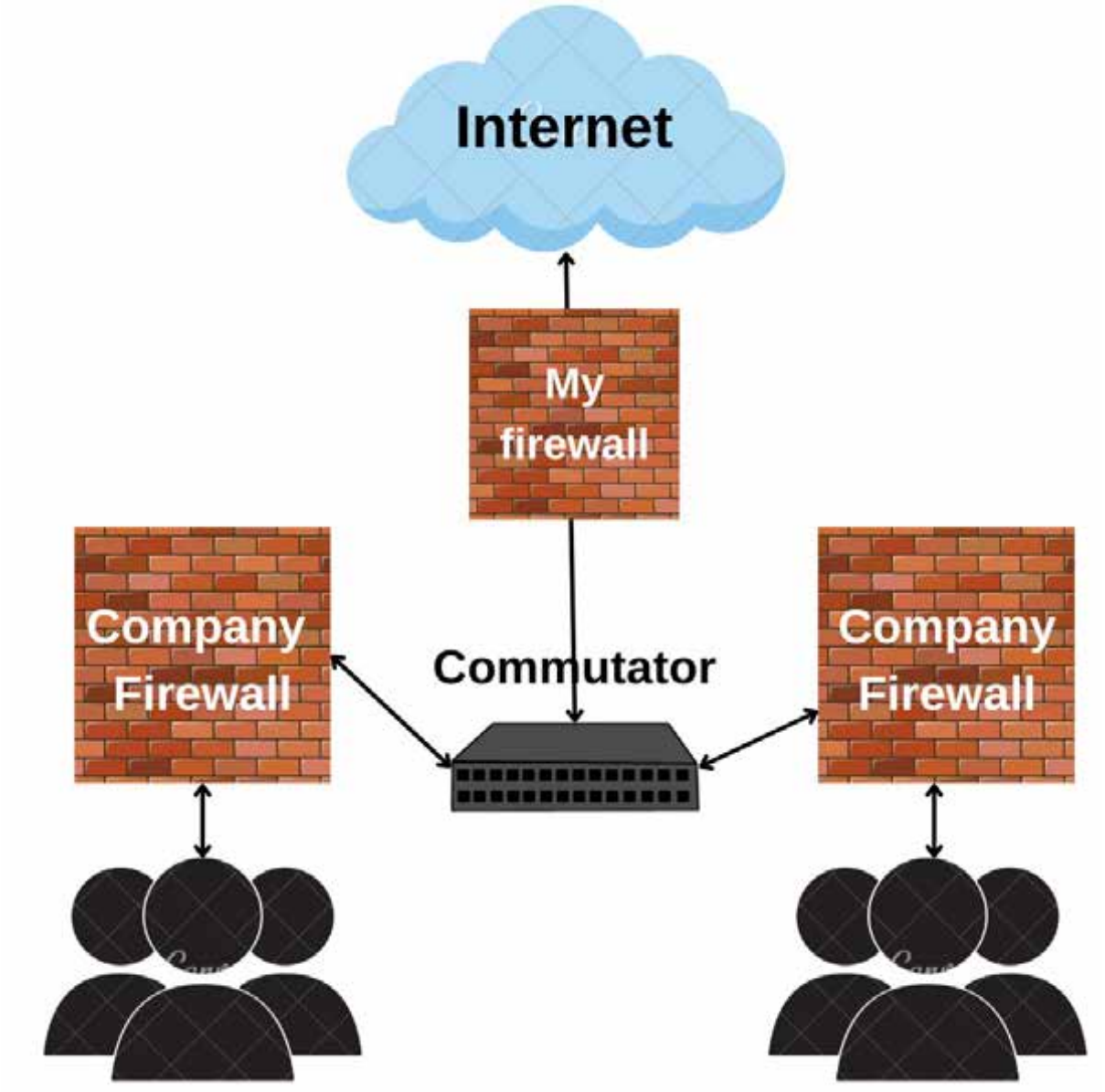

Рис. 4 Схема встановлення firewall

Даний брандмауер був налаштований на дозвіл усього трафіку та реєстрацію даних, що проходили через нього. Він не здійснював жодних втручань та не перешкоджав щоденній діяльності компаній, де він був встановлений.

Ми створили базу правил, що базувалася на ISSP (Information Systems Security Policy), для виклику тригера на основі отриманого трафіку. Також ми внесли деякі тригери найкращої практики на брандмауер, щоб ми могли виявляти такі події. Це тригери найкращих практик, наприклад номери кредитних карток, медичну інформацію та великі файли. Усі зареєстровані дані будуть розміщені у категорії, такі як Бізнес-інформація, Комплаєнс, Особисто-ідентифікована інформація тощо.

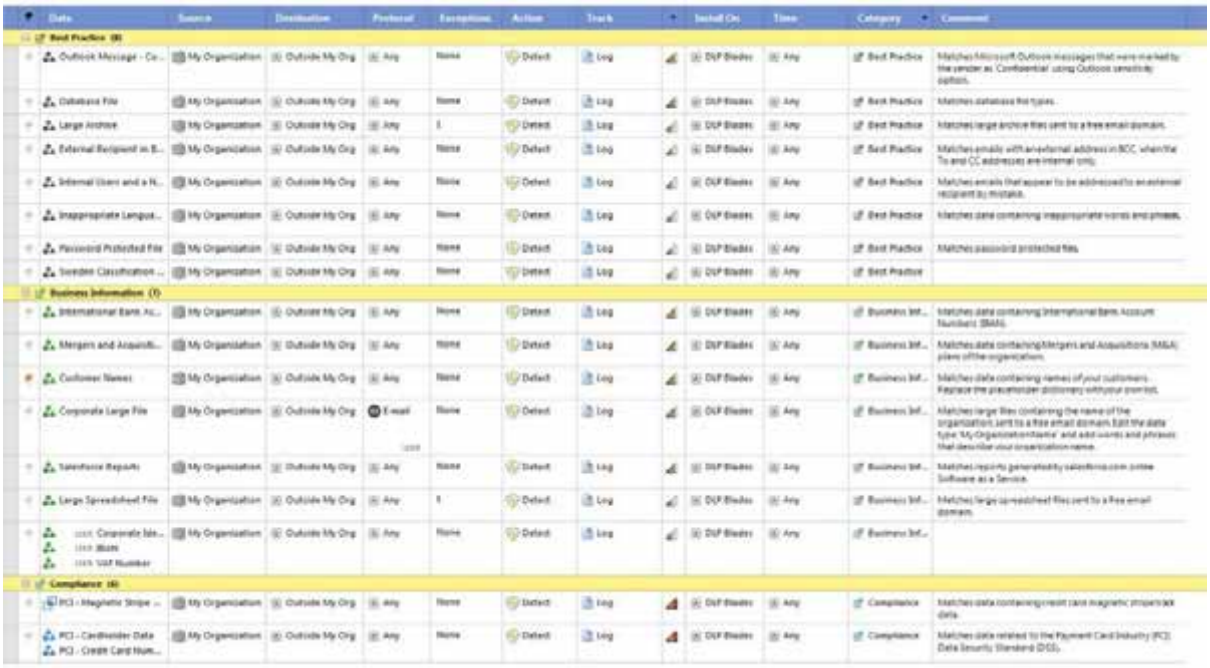

Рис. 5 DLP-правила

Брандмауер створює журнал інцидентів на основі створених тригерів. Цей список включає інформацію, отриману під час глибокого аналізу кожного окремого пакета, який проходить через брандмауер. Він проводить пошук по всім

даним, що передаються, даних, що були введені у форми та всього, що може бути представлено у вигляді тексту.

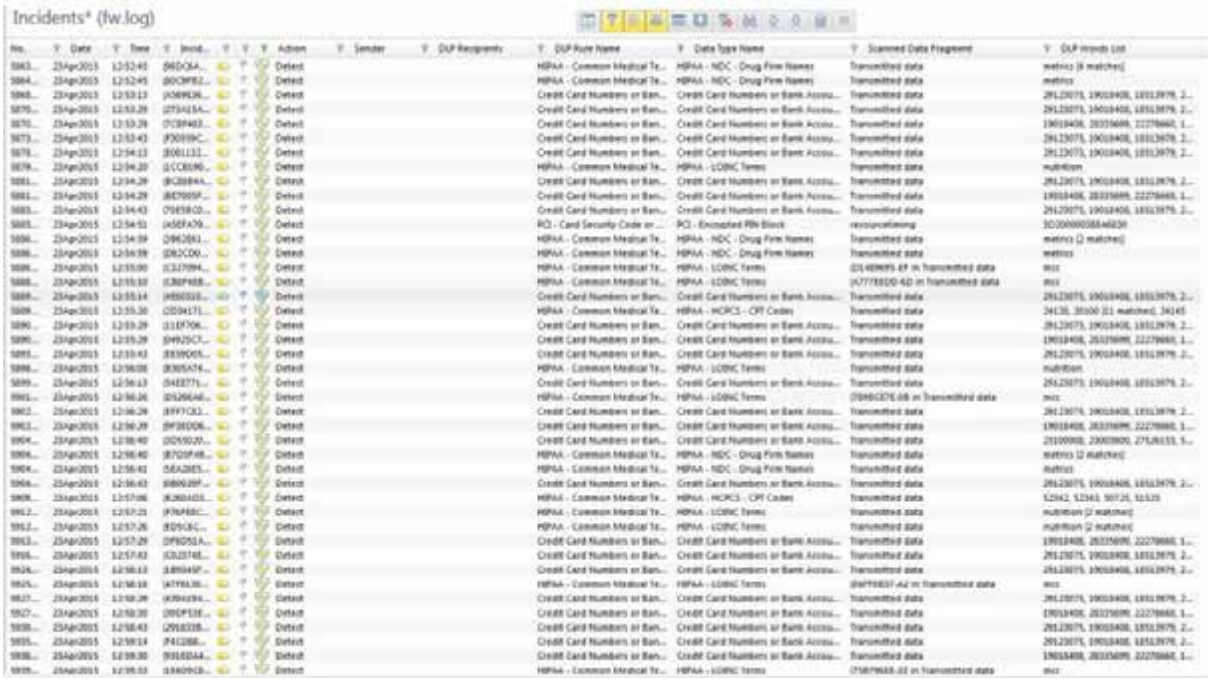

Рис. 6 Журнал(логи) брандмауера

З цього списку можна докладніше розглянути окремі інциденти для подальшого аналізу, щоб визначити, чи це справжній інцидент, чи хибний. Із цього ми вивчили, що ця частина є дуже важливою для адміністратора з безпеки, щоб налаштувати інформацію так, щоб в журналі залишалися лише справжні інциденти. Під час докладного аналізу інцидент буде занесений до журналу аудиту, оскільки переглядаючи інцидент, можна отримати конфіденційні дані і навіть читати листування або вкладення. Це також означає, що потрібно мати політику забезпечення безпеки, що визначає, хто може мати доступ до цих журналів і як їх обробляти. До цих журналів повинні мати доступ тільки найбільш надійні люди, адже у них зібрано всі приватні дані, а тому персонам зі злими намірами не потрібно буде їх шукати деінде ще.

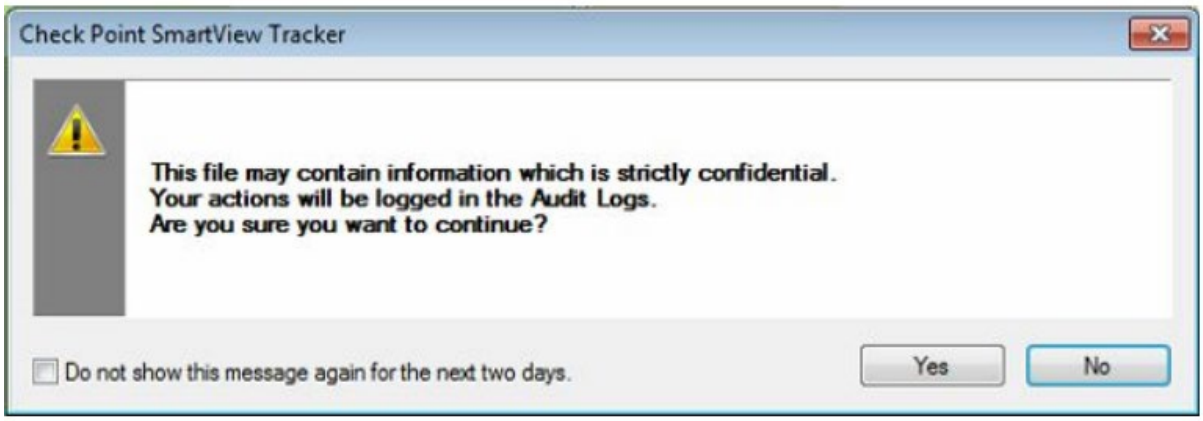

Рис. 7 Попереджувальне вікно

Детальний аналіз даних розкриває всю інформацію про те, які дані були відправлені, в який час, від кого і куди.

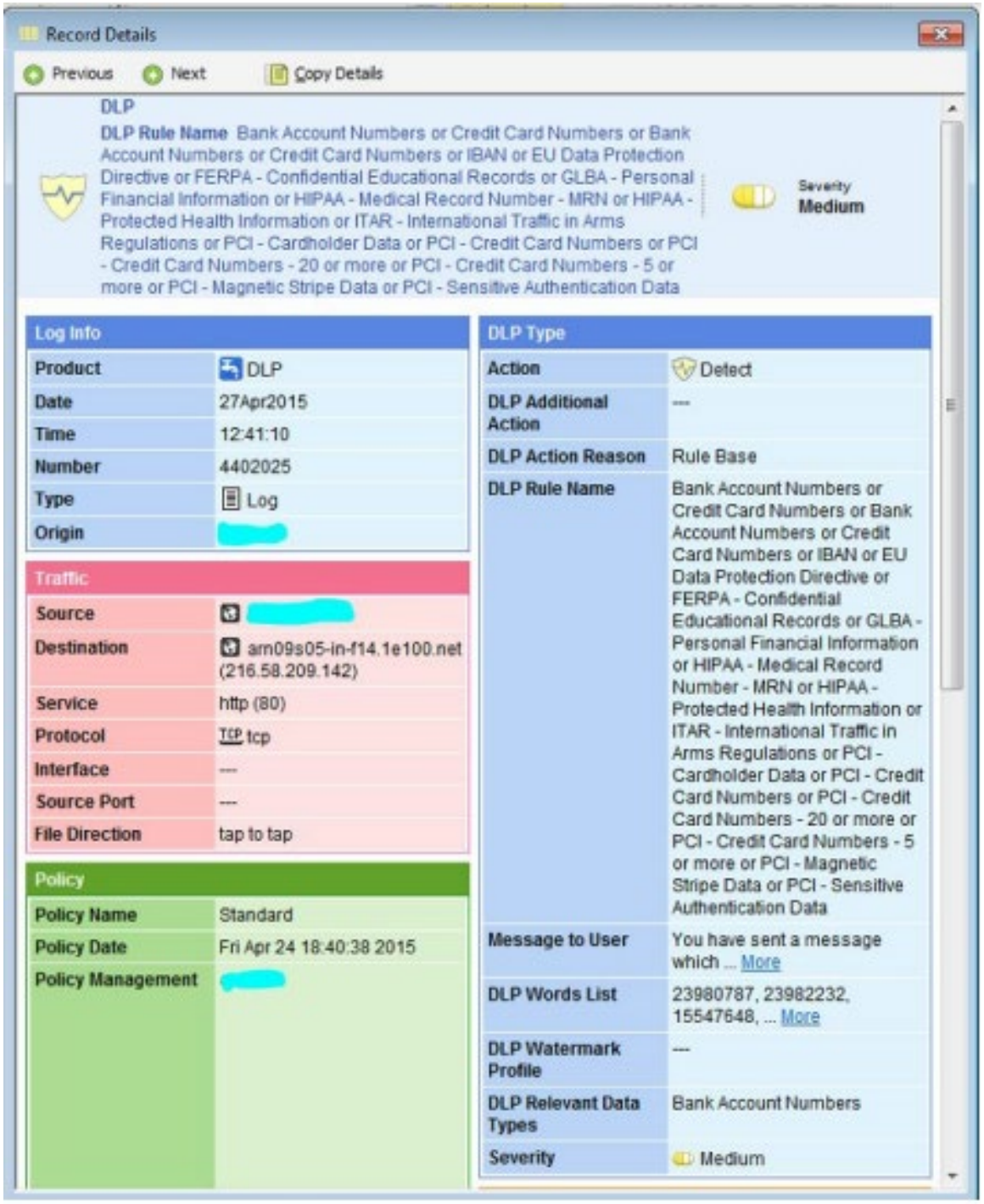

Рис. 8 Приклад детального перегляду інциденту

Це також показує інформацію про користувача, який відправив цю інформацію. Під час звичайної роботи ця інформація буде розміщена внутрішній мережі з підключенням до деякого джерела LDAP, наприклад, Microsoft Active Directory,

яке збиратиме як ім'я користувача, так і назву комп'ютера та іншу пов'язану інформацію.

Рис. 9 Інформація про відправника (1)

More	
Destination	arn09s05-in-f14.1e100.net (216.58.209.142)
Follow Up	Not Followed
Outgoing URL	http://www.google-analytics.com/collect
Proxied Source IP	[redacted]
Data Type Name	Credit Card Numbers or Bank Account Numbers
Data Type UID	{0B998C1F-890A-4E8D-8CED-0DBCC2F75C09}
DLP Categories	Compliance
DLP Transport	HTTP
Duplicate	No
Message Size	3646
Product Family	Network
Information	---

Рис. 10 Інформація про відправника(2)

Коли він виявляє інцидент витоку даних, він зареєструє передані дані або виконає захоплення пакетів, якщо вам цікава така інформація. Після цього ви можете переглянути дані; якщо це електронний лист, відкриється копія відправленого листа.

Рис. 11 Приклад "сирих" даних

3.2 Інтерв'ю

Зустрічі з компаніями-учасниками розпочиналися з інтерв'ю для кращого пізнання їх і створення бази щодо подальшого збору даних щодо трафіку. Ось список питань, які задавалися під час інтерв'ю і пояснення, чому саме такі питання.

кільки людей працює у галузі інформаційної безпеки?

Згідно з ISO 27002, в організації повинна бути структура інформаційної безпеки. Ми хотіли знати, чи мають організації таку структуру і скільки людей в ній беруть участь.

то відповідає за ISSP (Політику інформаційної безпеки)?

Згідно з ISO 27002, в політиці повинні бути визначені певні ролі. Ми хотіли знати, чи відповідає політика цим вимогам ISO і чи відображають відповіді на інтерв'ю їхню ISSP.

к оновлюється ISSP?

Існує багато причин, чому особи можуть не дотримуватися ISSP, тому ISSP повинна оновлюватися і відображати поточні практики (Kolkowska & Dhillon, 2013). SETA стверджує, що особи повинні бути обізнані з існуванням ISSP і поточними версіями. Згідно з ISO 27002, ISSP повинна існувати в організації і регулярно оновлюватися, щоб враховувати поточні загрози та вразливості. Ми хотіли знати, чи існує такий ISSP і як часто він оновлюється.

к ви поширюєте знання про ISSP?

Особи в організації завжди повинні бути обізнані з поточною версією ISSP для уникнення ризиків і вразливостей (Bulgurcu et al, 2010; D'Arcy et al, 2009). Ми хотіли знати, як особи сповіщалися про оновлення та чи були вони обізнані з поточною версією та процедурами безпеки.

к користувачі обізнані з ризиками, пов'язаними з витоком даних?

Особи часто недостатньо інформовані про загрози та загрози безпеки навколо них. Багато дослідників вважають необхідним навчати та тренувати осіб щодо загроз та способів їх управління. Ми хотіли знати, чи був реалізований цей процес.

к ви навчаєте користувачів зменшувати ризики?

Згідно з Bulgurcu, існує кілька способів донесення інформації стосовно ризиків. Такими способами є особистий досвід атак та відповідність правилам та регуляціям щодо безпеки, газети, журнали і т. д. Bulgurcu та D'Arcy вважають, що SETA повинна навчати осіб, як зменшувати ризики небезпеки. Ми хотіли

знати, чи користувачі отримували навчання з безпеки щодо правильної поведінки та чи було їм представлено стратегію від відділу IT.

ких регуляторних вимог організації зобов'язані дотримуватися?

Webspy стверджує, що існують два типи даних, які організації повинні захищати, щоб запобігти витоку даних: приватна інформація, або ж особисто ідентифікована інформація, та інтелектуальна власність, яка стосується активів організації, конфіденційних даних тощо. Ми хотіли знати, чи організація дотримується якихось регуляторних вимог, щоб створити тригери для брандмауерів на основі таких типів даних.

Звісно, я спробую покращити переклад. Ось ваш текст із виправленнями:

и ви маєте інформацію про випадки порушень безпеки, які сталися?

Знаючи, як працює процедура забезпечення безпеки, зловмисникам може вдатися видалити докази після себе, і організація може ніколи не дізнатися, що сталося порушення безпеки (Ахмад та ін., 2013; Бласко та ін., 2012; Чіверс та ін., 2009; Колвілл, 2009; Мур та ін., 2009; Уокер, 2008). Ми б хотіли дізнатися, чи вони мають інформацію про випадки порушень, як вони їх вирішують та як вони дізнаються про такі порушення.

кі будуть наслідки витоку інформації?

Знання мають свою вартість. Витік інформації має вплив на прямі витрати, а також непрямі витрати, такі як втрата репутації. Ми ставимо це питання, щоб дізнатися, чи компанії провели оцінку ризику та оцінили свої інтелектуальні активи.

кі дані ви вважаєте чутливими та не повинні залишати межі компанії?

Різні компанії мають різні види даних, які вважають чутливими. Компанія, що розробляє програмне забезпечення, зазначає, що такими даними є їхній вихідний код, банк може зазначити свої фінансові транзакції. Ми ставимо це питання, щоб дізнатися, чи розглядали вони цей аспект та чи є можливість сфокусуватись на саме таких подіях, для того щоб брандмауер реєстрував випадки витоку даних на підставі інформації, наданої цим питанням.

к ви дізнаєтеся про інцидент розголошення інформації?

Згідно з деякими виданнями, моніторинг є необхідним заходом безпеки, призначеним для зменшення випадків недобросовісного використання інформації, намірів на недобросовісне використання та випадкових інцидентів з боку осіб. Ми ставимо це питання, щоб дізнатися, чи в компаніях є якісь механізми виявлення витоку інформації, чи ж це ґрунтується лише на повідомленні про витік від когось.

кі кроки ви вживаєте для поліпшення культури безпеки?

SETA призначений для навчання осіб тому, на що слід звертати увагу, як це обробляти та водночас діяти згідно з ISSP. ISSP, SETA та моніторинг - це деякі контрзаходи проти порушень безпеки. DLP - це технічне рішення, призначене для запобігання витоку даних. Ми поставили це питання, щоб дізнатися, чи компанії пріоритезують питання підвищення свідомості про безпеку.

к ви реагуєте на внутрішні порушення безпеки?

Згідно з Chen, Ramamurthy, & Wen , особи менш схильні вчиняти порушення безпеки, якщо вони знають, що їх контролюють і їх покарають за такі дії. Також, надаючи винагороду тим, хто діє/працює в позитивний спосіб, більш схильно

уникають і навіть допомагають у запобіганні порушень безпеки. Ми хотіли дізнатися, який підхід обирають компанії в цьому питанні.

Компанія 1

Кейс 1 був проведений в муніципалітеті України. Муніципалітети є дуже відкритими та вільними організаціями, і більшість того, що вони роблять, не є конфіденційним. З іншого боку, справді чутлива інформація є дуже конфіденційною. Вони вирішують справи через соціальні служби, імміграцію та охорону здоров'я. Ми розпочали інтерв'ю питанням: Скільки людей працює із інформаційною безпекою? Відповідь на це питання була досить неоднозначною. У них є розподілена система роботи з інформаційною безпекою, де кожен відповідає за свої дії та повинен переконатися, що він обробляє чутливу інформацію правильним чином. У більш конкретній області вони не мають жодної особи, яка б працювала із інформаційною безпекою, щоб переконатися, що вона обробляється правильно. Вони несуть спільну відповідальність. Наступне питання було: Хто відповідає за ISSP? Навіть на це питання була неоднозначна відповідь. ISSP створюється всередині організації, але вона передається міській раді на затвердження чи відхилення. Коли вона затверджується, організація повинна дотримуватися її до тих пір, поки не буде доступний новий ISSP. Організація не може вирішувати політику самостійно; політика повинна пройти через міську раду. Організація, однак, може створити директиви. Третє питання було: Як оновлюється ISSP? В муніципалітеті не існує визначеного процесу або циклу оновлення ISSP. З огляду на велику кількість різних служб у муніципалітеті, потрібно враховувати багато різних потреб. Тому загальне правило полягає в тому, що все, що стосується роботи, допускається. ISSP визначає, що є найважливішим з точки зору забезпечення безпеки, тому він оновлюється, коли "хтось" бачить потребу оновити його через зміни в середовищі. Наступне питання було: Як розповсюджується знання про ISSP? В цій компанії ISSP підписується при прийнятті на роботу. Співробітники несуть

відповідальність за те, щоб знайти та пройти оновлені ISSP, які публікуються в Інтранеті і доступні всім співробітникам. В Інтранеті є функція, яка показує користувачеві, які документи були оновлені останнім часом. Пішли далі, ми поставили питання: Як користувачі усвідомлюють ризики, пов'язані із витоком даних? В організації немає навчання щодо свідомості про безпеку, тому це ґрунтується на здоровому глузді та на тому, що користувачі ставлять питання до служби технічної підтримки IT чи якомусь керівництву на цю тему. Після цього ми поставили питання: Як ви навчаєте користувачів зменшувати ризики? Як було сказано в останньому питанні, в організації немає навчання щодо свідомості про безпеку. Тому, навіть тут, організація базується на тому, що клієнти використовують здоровий глузд для застосування заходів безпеки. Сьогодні користувачі знають, що не слід натискати на посилання в електронному листі, якщо вони не знають від кого він, і що вони не повинні передавати свій пароль іншим особам.

Потім ми перейшли до розділу про попередні порушення, починаючи з питання: Які нормативні акти повинна дотримуватися організація? Оскільки це муніципалітет, він повинен дотримуватися законів та нормативних актів, що стосуються таких організацій.

Потім ми поставили питання: Чи відомо вам про які-небудь порушення, які сталися? Вони сказали, що не відомо про жодні витоки даних, які могли статися, але їх атакували DDoS-атаками та великими відключеннями. Вони зазначили, що навіть якщо вони не знають про події щодо витоку даних, вони досить впевнені, що деякі з них могли статися, але в них не було інструментів для їх запобігання чи виявлення таких порушень.

Наступним питанням було: Які наслідки має витік інформації? Наслідки для муніципалітету досить відрізняються від наслідків для приватної компанії. Наприклад, випадок, коли чутлива інформація витікає, не змусить когось переїхати в інший муніципалітет. Звісно, це призведе до поганої репутації. Для муніципалітету це також може призвести до розслідувань і штрафів.

Після цього ми перейшли до питання: Які дані ви вважаєте чутливими і які не повинні залишати територію компанії? Однією з причин цього питання є створення базового рівня для подій витоку даних, які повинні викликати сигнал для частини роботи щодо збору даних в рамках дисертації. Найчастіше чутливі дані - це особисто ідентифікована інформація. У них є інформація про всіх мешканців і використовується особисто ідентифікована інформація в їхній щоденній роботі, але ця інформація не повинна виходити за межі муніципалітету. Дані з соціального захисту в загальному чутливі, те ж саме стосується інформації з охорони здоров'я.

Наступним питанням було: Як ви дізнаєтеся, якщо дані витікають? У організації немає жодних інструментів, які можуть виявити витік інформації, тому бути передбачливим не можливо. Єдиний спосіб дізнатися про витік даних - це, якщо хтось інший повідомить їм про це. До моменту інтерв'ю такого не траплялось.

Далі ми поставили питання: Які дії ви вживаєте для поліпшення культури безпеки? Робота над культурою безпеки у свій час була важливою для них, але через обмеження у часі вона не була пріоритетом. Проте вони працюють над загальною культурою: бути ввічливими та скромними у стосунках одне з одним та людьми поза організацією, тому мають надію, що це також допоможе в поліпшенні культури безпеки.

Останнім питанням, яке ми поставили, було: Як ви реагуєте на внутрішні порушення? Якщо їм стає відомо, що працівник спричинив витік даних, він отримає письмове попередження. Якщо це повторюється, це може призвести до дисциплінарних заходів чи навіть правових заходів.

Компанія 2

Кейс 2 був проведений у міжнародній компанії-розробнику програмного забезпечення, яка має офіси по всій Європі. Компанія має значну частку ринку в своєму сегменті і потребує захищати інтелектуальну власність, а також

інформацію про клієнтів та дорожню карту продукту. Ми розпочали інтерв'ю питанням про кількість людей, які працюють з інформаційною безпекою.

Організація не має спеціаліста, який виключно працює з інформаційною безпекою, але декілька осіб мають інформаційну безпеку в своєму описі робіт. Їх завданням є створення ISSP та забезпечення безпеки свого продукту на необхідному рівні.

Наступним питанням було "Хто відповідає за ISSP?" Менеджер IS/IT відповідає за те, щоб в організації був ISSP, але завдання створення та оновлення його протягом життєвого циклу розподіляється між багатьма.

Питання номер 3 було "Як оновлюється ISSP?" У компанії ISSP оновлюється за потреби, коли хтось розуміє, що ISSP не покриває деякі елементи, або якщо з'являється певний випадок і аналіз показує, що ISSP не вистачає для роботи в актуальному середовищі. Якщо потрібно оновити ISSP, це робить одна особа у якості керівника проекту. Не існує визначеного життєвого циклу для ISSP.

Наступним питанням було "Як ви поширюєте знання про ISSP?" Під час процесу адаптації нові працівники проходять вступну програму, яка включає, серед іншого, ISSP. Звісно, нові працівники повинні підписати ISSP, отримавши доступ до IT-засобів. ISSP доступний користувачам через інструмент управління документами. Проблема полягає в тому, що зовнішні консультанти не мають доступу до системи управління документами. Якщо створюється нова версія ISSP, про це інформується у корпоративному інтранеті.

Далі ми поставили питання "Як користувачі обізнані з ризиками, пов'язаними з витоком даних?" Це також виконується під час початкового процесу адаптації. Наразі не існує навчальних програм з питань безпеки через обмеження часу, тому більше інформації, аніж наданої під час адаптації, працівники не отримують.

Наступним було "Як ви навчаєте працівників зменшувати ризики?" Це також включається в адаптаційний процес в усній формі. Навчання проводяться у випадках, коли компанія розуміє, що працівникам недостатньо обізнаності. Як

правило таке розуміння приходить, коли стається певний інцидент. Крім цього, компанія покладається на здоровий глузд, більшість користувачів мають високу освіту в галузі IT.

Потім ми перейшли до розділу про попередні порушення, розпочавши з питання: "Яких правил відповідності повинна дотримуватися організація?" У цій компанії немає жодних правил відповідності, які їй потрібно дотримуватися.

Потім ми запитали: "Чи вам відомо про якісь порушення, які сталися?" Відповіддю була згадка про декілька критичних випадків, але це були атаки DDoS і відключення. На даний момент компанія не має жодних випадків витоку даних, наскільки їй відомо.

Наступним питанням було: "Яким може бути вплив витоку інформації на компанію?" Це питання було включено в оцінку ризиків, яку провела компанія, і вплив вказано у зменшенні довіри на ринку, в залежності від серйозності це може призвести навіть до втрати клієнтів або штрафів.

Після цього ми перейшли до питання: "Які дані вважаються конфіденційними і не повинні залишати приміщення компанії?" Однією з причин цього питання є створення базового рівня тригерів для DLP-системи. Компанія тісно співпрацює зі своїми клієнтами, тому інформація про клієнтів є конфіденційною. Вони заробляють, розробляючи програмне забезпечення, тому важливо зберігати вихідний код в безпеці, головним чином через втрату репутації у разі його втрати.

Наступним питанням було: "Як ви дізнаєтеся про випадки витоку даних?" На сьогоднішній день у компанії немає системи для виявлення витоку даних. Єдиним способом дізнатись про такий інцидент є випадковість, тобто коли працівник робить якусь роботу та випадково помічіє підозрілу активність, або якщо хтось інший повідомляє компанії, що дані витекли.

Потім ми задали питання: "Які дії ви вживаєте для поліпшення культури безпеки?" Це також відбувається під час періоду адаптації. Процес адаптації включає одноособовий огляд, який також охоплює політику та практики безпеки.

Під час цього огляду користувачі отримують вступ до процедур з безпеки. Якщо всі дотримуються цих процедур, то культура безпеки буде непоганою. Після завершення процесу адаптації сервісний центр компанії проводить непримусові навчання користувачів, використовуючи не палку, а пряник. Культуру неможливо створити силою.

Останнім питанням, яке ми задали було: "Як ви реагуєте на внутрішні порушення?" Якщо повідомляється про внутрішнє порушення, коли хтось створив ситуацію витоку даних, це стає справою для відділу кадрів. Залежно від серйозності порушення користувачу надається усна або письмова догана. Якщо та ж сама особа вчиняє декілька порушень, її навіть можуть відправити у відставку.

ISSP

3.3.1 Компанія 1

Компанія 1 (муніципалітет), має дуже відкриту політику, де ніщо не є неприпустимим. Уряд загалом не повинен проводити цензуру, і це та лінія, якою керується компанія 1.

Загальне правило полягає в тому, що все, що робить користувач, може бути відстежувано та переглянуто, тому етика та мораль мають важливе значення. Головна причина такої політики - обмежити розлади в інформаційних системах, щоб кожен міг використовувати системи для виконання своїх завдань.

Політика визначає, що інформаційні системи можуть використовуватися лише для робочих завдань, і працівник повинен зберігати облікові записи та паролі в секреті.

Далі політика зазначає, що працівник повинен діяти так, щоб запобігти саботажу або розладам для інших користувачів та центральних систем. Один з підходів до

цього полягає в тому, що користувачам заборонено підключати обладнання, яке не управляється відділом IT, до мережі.

Копіювання або розповсюдження матеріалів, що захищені авторським правом, не дозволено, якщо власник даних не схвалив це, і розповсюдження матеріалів взагалі може бути обмежено у разі необхідності з фінансових причин.

Крім того, політика визначає, що відділ IT зберігає журнали всього трафіку протягом трьох місяців, щоб мати можливість вирішувати поточні завдання або усувати неполадки, а також відслідковувати підозрілі витоки інформації. Вони також мають право вимкнути доступ через порушення безпеки і зобов'язані повідомити про це керівнику працівника, який вирішує, як вирішити порушення.

Політика також зазначає, що відділи соціального забезпечення та IT зобов'язані впроваджувати контроль доступу до інформації, яка підпадає під український закон про захист персональних даних.

Угода про нерозголошення, яка використовується в соціальному забезпеченні та освітніх послугах, зазначає, що інформація, яка дозволяє ідентифікувати особу, не повинна розголошуватися, якщо особа або її родичі отримають шкоду, або ж просто не погоджуються з цим. Нарешті, зазначається, що Угода про нерозголошення охоплює частину областей, які розглядаються службами соціального забезпечення та освітніми послугами.

3.3.2 Компанія 2

Компанія 2 - приватна компанія і розробила кілька різних документів політики, які в сумі створюють їхній набір політик щодо інформаційної безпеки системи.

Першою є політика облікового запису користувача, яка визначає, що облікові записи є особистими, і користувач повинен зберігати їх у безпеці, використовуючи пароль із 12 символів, який важко вгадати і який залишається конфіденційним. Також вказується, що користувач не повинен ніколи ділитися своїм паролем, і якщо він підозрює, що хтось отримав доступ до нього, користувач повинен негайно змінити його. Важливо не залишати запису пароля

у небезпечному місці або зберігати його так, щоб інші могли зрозуміти, що це пароль.

Наступною є політика ПК, яка включає в себе правила стосовно того, що може бути встановлено на комп'ютер, заборону зберігання авторських матеріалів на комп'ютері і заборону підключення особистого обладнання до корпоративної внутрішньої мережі компанії. Варто відзначити, що у них є окрема фізична мережа, куди користувачі можуть підключати інше обладнання. Працює ця мережа на протоколі 802.1x для покращення безпеки на цьому пункті. Політика також зазначає, що користувачам заборонено впроваджувати технічні рішення, які можуть піддавати ризику корпоративну безпеку, принаймні без погодження з відділом IT. Політика навіть зазначає, що відвідування веб-сайтів із незаконним, непристойним або образливим матеріалом заборонено.

Деяким користувачам надаються права локального адміністратора на їх комп'ютерах, і для них існує окрема політика, яку слід дотримуватися. Ця політика визначає, що встановлення авторського програмного забезпечення без корпоративного серійного номера не дозволено, а також встановлення програмного забезпечення, яке не відноситься до роботи. Також визначається, що заборонено вимикати або вносити зміни до робочого антивірусного клієнта, а також змінювати компоненти попередньо встановленого образу Windows.

Останньою політикою, до якої ми маємо доступ, є загальна Політика інформаційної безпеки системи. Ця політика починається з визначення структури безпеки компанії. Немає окремої відповідальної особи за питання безпеки, а скоріше група осіб, які, як сказав керівник відділу IT, є дуже відповідальними.

Політика починається з визначення основних принципів. Основним принципом є те, що безпека ґрунтується на потенційних збитках, які можуть виникнути внаслідок деяких подій. Крім того, вона визначає, що про всі інциденти повинно бути повідомлено, вони повинні дотримуватися правил і регламентів, і всі системи повинні мати визначеного власника, який відповідальний за впровадження, використання і аудит засобів безпеки.

Далі в політиці визначаються основні правила, які вказують, що все обладнання призначене тільки для робочих завдань, всі пристрої повинні мати встановлені останні патчі безпеки та повинні бути схвалені відділом IT перед підключенням до мережі.

Потім є розділ про облікові записи користувачів. На основі інформації в політиці облікових записів користувача, на яку звертаються в ISSP, цей розділ може здатися зайвим. Але деякі аспекти відрізняються, такі як те, що облікові записи користувачів, які не використовуються протягом 6 місяців, будуть вимкнені, і через 6 місяців після цього вони будуть видалені. У цьому розділі також зазначається, що заборонено відтворення даних у списки, флешки, CD-ROM або зберігання на лаптопах. Тут зазначено, що витік даних заборонений!

Після цього вони вказують, що в підрозділі IT-відділ розповсюджує захищений паролем екранний заставка, який не повинен змінюватися, і кожного разу, коли ви залишаєте комп'ютер, ви повинні блокувати робочу сесію. В кінці робочого дня ви повинні вимкнути комп'ютер.

У наступному розділі зазначається, яку інформацію заборонено зберігати на зберіганні, підключеному до мережі. Заборонена інформація включає образливий та образливий матеріал, авторське програмне забезпечення без дійсної ліцензії, матеріали, які захищені авторським правом, такі як музика і відео, не робочі відео, ігри і, нарешті, особисті файли, такі як фотографії і т. д. Проте вони не зазначають жодних вказівок щодо обробки чутливої інформації.

Наступний розділ зосереджується на вірусах і тому, як їх запобігати, а також як не використовувати електронну пошту у відношенні до чуток, листів-цепочок і подібних. Також зазначається, як реагувати, якщо ви підозрюєте інфікування вірусом. Ці рекомендації включають відключення комп'ютера від мережі, щоб обмежити поширення вірусу, а також звернення до служби підтримки IT. Наступні розділи розглядають різні типи поведінки. Перший визначає, який контент треба запобігати в Інтернеті. Знову вказується на важливість не встановлювати програмне забезпечення, яке надає компанія, і запобігати завантаженню вірусами.

Наступний розділ стосується електронної пошти, вказуючи, що заборонено автоматично пересилати всю електронну пошту на зовнішні скриньки, такі та ін. Також зазначається, що надавати електронну адресу на веб-сайтах або брати участь в розсилках заборонено, якщо це не стосується роботи.

Наступний розділ стосується захисту ноутбука. Зазначається, що шифрування жорсткого диска необхідне, якщо користувач має чутливу інформацію на ноутбуці. Важливо також безпечно зберігати та переносити комп'ютер і негайно повідомляти про крадіжку службі підтримки IT.

Далі йде розділ про мобільні пристрої. У політиці зазначено, що зберігання чутливої інформації на мобільних пристроях не дозволяється, і синхронізація електронної пошти допускається лише на певних пристроях, які схвалені відділом IT.

Наступний розділ стосується віддаленого доступу. Доступ до VPN надається співробітникам за двофакторною аутентифікацією, за винятком електронної пошти, яка доступна через веб-сайт SSL. Компанія також має VPN-тунелі до клієнтів, для яких використовується AAA, а також обмеження доступу тільки до того, що потрібно клієнтам. Паролі для систем клієнтів зберігаються в зашифрованій базі даних з повним відстеженням того, хто має доступ до пароля.

Політика також містить вказівки щодо фізичної безпеки, такі як підтримання чистоти на столі, не залишання документів на принтері та не залишання чутливої інформації в конференц-залах.

Останнім заявленням політики є класифікація інформації. Компанія створила свою систему класифікації. Інформація класифікується як публічна, внутрішня або конфіденційна, а користувачі, які мають до неї доступ, класифікуються як публічні користувачі, внутрішні користувачі, партнери або клієнти.

Завершальним положенням політики є наслідки недотримання політики. Це призводить до звернення до менеджера, що відповідальний за працівника, відкликання дозволів та усного або письмового зауваження чи попередження. Для більш серйозних випадків це може призвести до звільнення, відставки та повідомлення до поліції. Викрадення інформації є прикладом цих більш серйозних випадків.

3.4 Звіт по трафіку

3.4.1 Компанія 1

Брандмауер, який ми встановили, працював в живому середовищі у муніципалітеті протягом 9 днів. 7 з них були робочими днями. Протягом цього часу було відправлено майже 2,2 ТБ даних до брандмауера, де спрацювало 303 532 можливих подій витоку даних. Система запобігання втрати даних (DLP) від брандмауера створила ці події:

Type of data	Number of events
PCI – Card Security Code	298 619
Credit Card Numbers or Bank Account Numbers	3494
Programming language lines (Source Code), such as C, C++, C#, JAVA	541
PCI – Expiratoin Date	521
PCI – Encrypted PIN Block	348
UKR Classification Code	9
Total	303 532

Табл. 2 Приклад звіту DLP брандмауера (Компанія 1)

Різні події від брандмауерів розділяються на різні категорії, як показано в таблиці вище.

Категорія "PCI - Код безпеки карти" є типом даних, що складається з чотирьохзначних чисел. Тому кожного разу, коли дані проходили через брандмауер і виявляли чотиризначне число, він реєстрував подію, незалежно від інших обставин. Це частина найкращих практик щодо відповідності PCI, але оскільки муніципалітет не обробляє кредитні картки, ми відкидаємо всі ці події як помилкові позитиви. Помилковий позитив - це подія, що створюється на основі даних, які неправильно інтерпретовано. Ідеальним прикладом буде саме цей випадок.

Для класифікації даних як "Номери кредитних карт або номери банківських рахунків" брандмауер шукає послідовність чисел, яка може бути номером кредитної картки або номером банківського рахунку.

Категорія "Рядки мов програмування (вихідний код), такі як C, C++, C#, JAVA" використовується, коли брандмауер виявляє блок даних, який відповідає синтаксису найбільш використовуваних мов програмування.

PCI - Термін дії" - це категорія, яка використовується при оплаті за допомогою кредитної картки. При введенні даних своєї картки ви повинні вказати термін дії вашої кредитної картки у форматі mm/yy. Тобто дві цифри для місяця, за якими слідує коса риска, і потім дві цифри для року. Тож, якщо термін дії кредитної картки закінчується в квітні 2015 року, термін дії буде записано як 04/15. Тепер всі дані, що складаються з числа, меншого або рівного 12, за яким слідує коса риска і дві цифри, будуть віднесені до цієї категорії.

Категорія "PCI - Зашифрований PIN-блок" складається з зашифрованих PIN-кодів, які відповідають одному зі стандартів ISO. Усі вони представляють дані у вигляді чотирьох блоків по чотири шістнадцяткових цифри. Отже, приклад потоку даних виглядає так: "1412 348D 665A C5A3". Кожного разу, коли брандмауер бачить такий патерн, він реєструє його як категорію "PCI - Зашифрований PIN-блок". Це також частина найкращих практик для відповідності стандарту PCI DSS.

"Українські терміни класифікації" - це терміни, які використовуються в шведській військовій та урядовій сферах для класифікації даних.

Нижче ви бачите графічне представлення розподілу значень по різних категоріях.

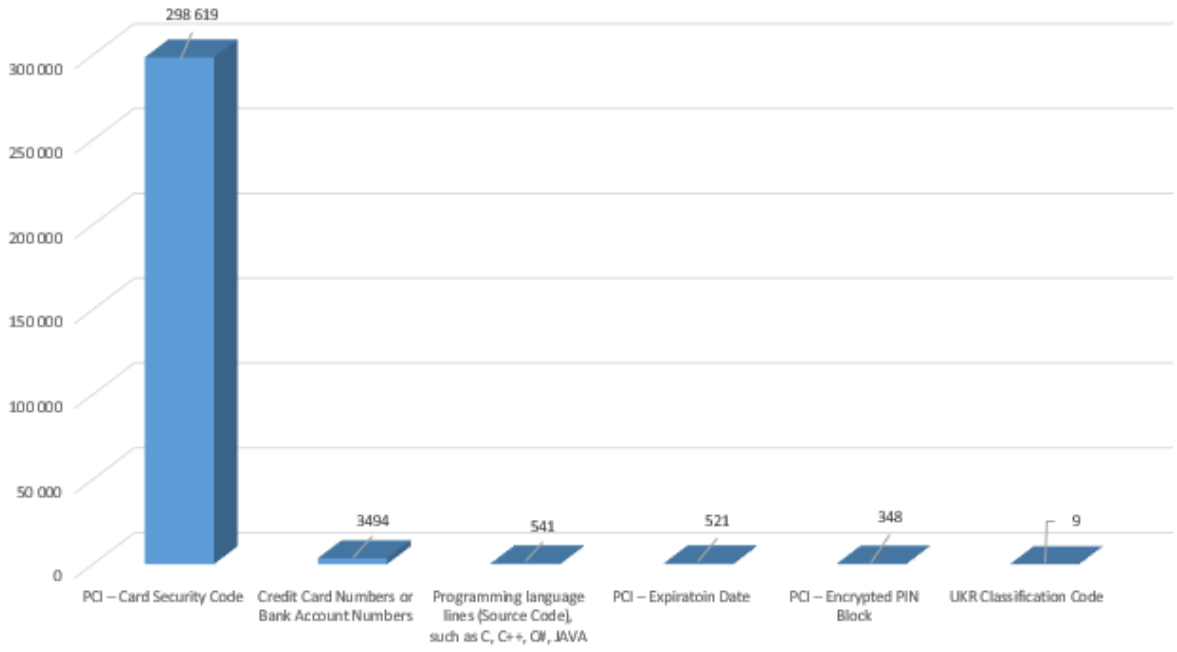

Рис. 12 Розподіл значень інцидентів по різних категоріях (Компанія 1)

Після самостійного аналізу, нами було виявлено ще низку інцидентів з витоком даних.

Type of data	Number of events
Social Security Number, Account number, Salary	9
Social Security Number	14
List of more than 10 Social Security numbers	1
Username and Password	1
Medical Information	3
Social services information	3

Табл. 3 Самостійний аналіз витоку даних (Компанія 1)

Отже, загалом ми виявили 31 порушення політики інформаційної безпеки. Завдяки великій кількості повідомлених подій і обмеженому знанню компанії ми не можемо гарантувати, що це все. Крім того, дані, які зашифровані, не реєструються через відсутність можливостей дешифрування для категоризації. Ще одною корисною інформацією є те, що всі ці порушення були відправлені по електронній пошті.

3.4.2 Компанія 2

Брандмауер був встановлений в компанії 2 протягом 10 днів. Протягом цих днів було лише 5 звичайних робочих днів, але компанія надає підтримку для клієнтів цілодобово, 7 днів на тиждень, 365 днів на рік. У компанії є багато брандмауерів, які покривають різні частини бізнесу, але ми розглядали лише брандмауер, який контролює зовнішній доступ до Інтернету. Інші брандмауери обробляли доступ до встановлень на клієнтів, VPN-тунелі до філійних офісів тощо. Протягом цих 10 днів брандмауер обробив 500 гігабайт трафіку. Система запобігання втрати даних (DLP) зареєструвала наступні події:

Type of data	Number of events
Login Credentials	41
IPv4 Address – 20 or more	20
SQL Queries	13
Business Plan Terms	6
Internal Users and a New External Recipient	5
PCI – Cardholder Data	3
Business Plan Topics	2
Source Code Scripts	2
External Recipient in BCC	2
Source Code – JavaScript	2
Database File	2
Active Directory or LDAP Entries	2
Source Code	2
MAC Address	2
Other	14
Total	118

Табл. 4 Приклад звіту DLP брандмауера (Компанія 2)

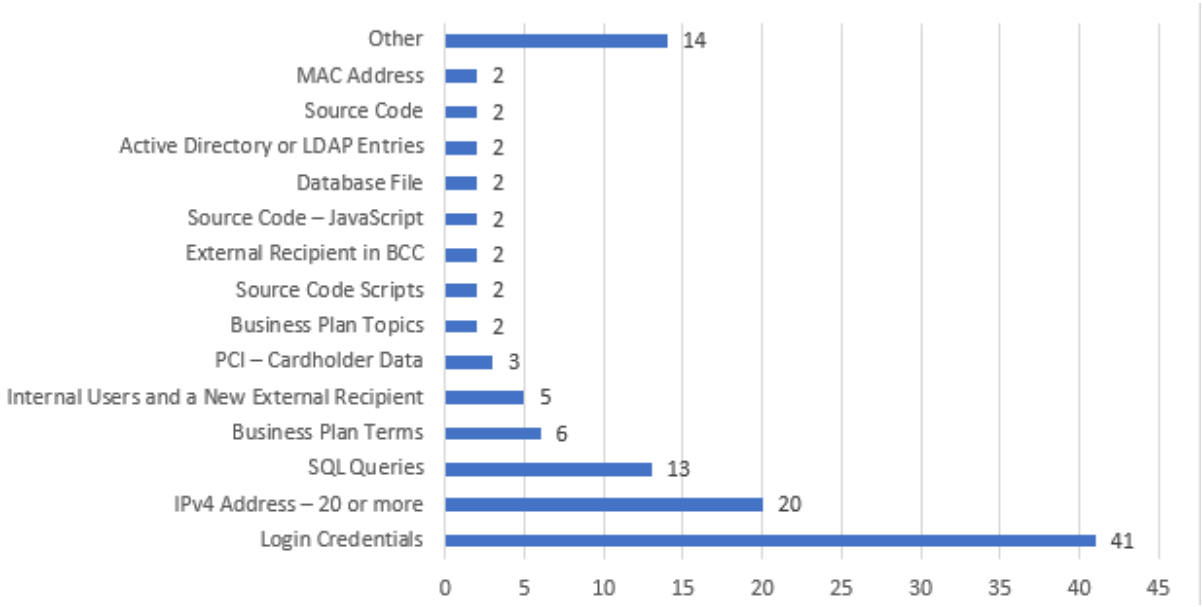

Рис. 13 Розподіл значень інцидентів по різних категоріях (Компанія 2)

У категорії "Логін і пароль" брандмауер шукає відомі способи запису логіна та пароля, а також шукає ключові слова "login" і "password". Саме в цій категорії ми знайшли всі. Ми також бачили, як зовнішні партнери та клієнти надсилали свої логіни та паролі у дану компанію, проте ми не класифікували їх як випадки

витоку даних для нашої компанії. Проте одне, що ми виявили, полягало в тому, що ці дані надходили через електронну пошту, і відповіді на ці листи все ще містили інформацію для входу.

Категорія "IPv4-адреси" шукає послідовності чисел із крапками між ними. Більшість з цих даних взагалі не були IP-адресами, а просто бінарними даними. Деякі з них були IP-адресами, але самі по собі IP-адреси не є чимось чутливим. Якщо б вони містили імена серверів або функції, то ситуація була б іншою. Ми не можемо сказати, що це були випадки витоку чутливих даних.

Компанія отримує свій дохід завдяки створенню програмного забезпечення зі сховищем даних SQL. Вихідний код і запити SQL є частиною інтелектуальної власності компанії, а отже дуже важливі для захисту. У наших випадках це були приклади загального вихідного коду, який не розкривав чутливих даних, тому ми також не класифікували їх як випадки витоку даних.

Після самостійного аналізу ми виявили ще деякі випадки витоку даних.

Type of data	Number of events
Username and Password	16

Табл. 5 Самостійний аналіз витоку даних (Компанія 2)

АНАЛІЗ ДАНИХ. РЕЗУЛЬТАТИ

Пошук за шаблонами - інтерв'ю

4.1.1 Компанія 1

Питання	Відповідь	Політика компанії
Скільки людей працює у інформаційній безпеці?	Немає призначених персон та ролей	Немає
Хто відповідальний за ISSP?	Немає призначених персон та ролей. Місцева адміністрація вирішує.	Немає
Як часто оновлюється ISSP?	«на льоту»	Не вказано де що і як
Як розповсюджуються знання про ISSP?	Під час періоду адаптаці (при прийомі на роботу). Подальші оновлення - через Інтранет	Не вказано
Як працівники дізнаються про ризики, пов'язаних із витоком даних?	Здоровий глузд та засоби підтримки IT	Не вказано
Як проводяться навчання по зменшенню ризиків?	Засоби підтримки IT	Не вказано
Яких регуляторних норм повинна дотримуватись організація?	Законодавство щодо архівування, обробки інформації про пацієнтів та особисто ідентифікованої інформації.	Політика зазначає, що муніципалітет впровадив контроль доступу відповідно до закону про інформацію про пацієнтів.
Чи знаєте ви про випадки витоку даних?	Ні	
Яким буде наслідок витоку даних?	Розслідування та штрафи	Дана інформація повинна бути вказана у оцінках ризиків
Які данні ви вважаєте конфіденційними?	Особиста інформація, інформація на медичну тему	Політика стверджує, що деяка інформація з соціальних служб повинна залишатися конфіденційною.
Як ви дізнаєтесь про випадки витіканян даних?	Усно	

Які кроки ви приймаєте для покращення культури безпеки?	Робота над загальними культурними рисами у надії, що вони матимуть вплив і на культуру безпеки.	
Як ви справляєтесь з інцидентами інсайдерства?	Письмова догана. При повторному інциденті – правові рішення.	

Табл. 6 Аналіз відповідей на інтерв'ю та політики компанії (Компанія 1)

Є одне запитання, яке показує неузгодженість між політикою компанії та інтерв'ю, а саме частина, яка стосується конфіденційної інформації (питання 10). Політика лише стверджує, що деяка інформація з соціальних служб повинна залишатися конфіденційною, тоді як в інтерв'ю було виявлено, що інші елементи інформації також повинні бути збережені.

Відповіді в інтерв'ю свідчать про наявність деяких неформальних політик. Декілька пунктів було наведено під час інтерв'ю, які не згадані в політиці. Питання, які стосуються організації з питань безпеки (питання 1 і 2), мали нечітку відповідь під час інтерв'ю, проте й не були вказані в політиці компанії. Те ж саме стосується інформації про те, як оновлюється ISSP, як розповсюджується знання про ISSP та навчання щодо свідомості про безпеку (питання 3-6). Питання щодо звітності, роботи над культурою та обробки інцидентів (питання 11-13) також були виокремлені під час інтерв'ю, але не були згадані в політиці. Питання 7 щодо відповідності регуляціям були включені в політику (хоча б щось).

4.1.2 Компанія 2

Питання	Відповідь	Політика компанії
Скільки людей працює у інформаційній безпеці?	Є одна відповідальна за це людина. Працює вона part-time.	Немає
Хто відповідальний за ISSP?	IT менеджер	Відділ прийняття рішень
Як часто оновлюється ISSP?	«на льоту». Коли потрібно	Не вказано де що і як. Проте це вже застаріла інформація
Як розповсюджуються знання про ISSP?	Під час періоду адаптаці (при прийомі на роботу). Подальші оновлення - через Інтранет. Через систему управлінян документами.	Через систему управління документами
Як працівники дізнаються про ризики, пов'язаних із витоком даних?	Під час адаптації. Далі SETA тренінги.	Не вказано
Як проводяться навчання по зменшенню ризиків?	Під час адаптації. Засоби підтримки IT	Не вказано
Яких регуляторних норм повинна дотримуватись організація?		
Чи знаєте ви про випадки витоку даних?	Ні	
Яким буде наслідок витоку даних?	Штрафи, втрата довіри клієнтів, доходу	
Які данні ви вважаєте конфіденційними?	Особиста інформація, вихідний код	Класифікація даних згадується в політиці, але не наводяться конкретні типи даних.
Як ви дізнаєтесь про випадки витіканян даних?	Усно	

Які кроки ви приймаєте для покращення культури безпеки?	Навчання під час адаптації. Через службу підтримки IT.	
Як ви справляєтесь з інцидентами інсайдерства?	Письмова або усна догана. При повторному інциденті – правові рішення та звільнення.	

Табл. 7 Аналіз відповідей на інтерв'ю та політики компанії (Компанія 2)

Під час цього інтерв'ю не було виявлено значних відмінностей між інтерв'ю та політикою. Деякі питання були відповідним чином розглянуті під час інтерв'ю, навіть якщо це не було враховано в політиці. Це свідчить про наявність якоїсь неформальної політики або вказівок.

Частина, яка стосується роботи щодо свідомості про безпеку (питання 4-6), в цілому включається в процес прийому на роботу. Про це не згадується в політиці. Політика також не відображає результати ризик-оцінки, яку провела компанія 2.

Залишкові питання узгоджуються з політикою, і ми висловлюємо вдячність компанії за їх роботу з проведення ризик-оцінки.

Пошук за шаблонами – трафік

4.2.1 Компанія 1

Тип даних інциденту	Політика компанії
Social Security Number, Account number, Salary	Не вказано, що це конфіденційні дані
Social Security Number	Не вказано, що це конфіденційні дані
List of more than 10 Social Security numbers	Не вказано, що це конфіденційні дані
Username and Password	Не вказано, що це конфіденційні дані
Medical Information	Такі дані вважаються конфіденційними
Social services information	Такі дані вважаються конфіденційними

Табл. 8 Аналіз тригерів трафіку та політики компанії(Компанія 1)

Політика компанії визнає як конфіденційну інформацію лише медичну та соціальну інформацію. Інтерв'ю показало, що існують інші типи даних, які також є конфіденційними і не повинні покидати компанію. За результатами аналізу трафіку, на якому ми виявили 32 інциденти, лише 6 з них були типами даних, які відповідно до політики вважаються конфіденційними, тоді як 26 інцидентів відносяться до типів даних, які не згадані в політиці. Це становить понад 81 відсоток інцидентів, де типи даних, що не згадані в політиці як конфіденційні, стали предметом витоку.

Згідно з нашим концептуальним каркасом витік даних є або навмисним через намір користувача не виконувати правила, або ненавмисним на основі свідомості користувача щодо безпеки. Їхній спосіб передачі даних зовнішньому партнерові з відділу кадрів (HR) не враховує, як обробляти конфіденційні дані в безпечний спосіб. Під час нашого спілкування з компанією виглядало так, ніби це є суб'єктивним стандартом, і той спосіб передачі конфіденційних даних (номери соціального страхування, номери банківських рахунків та зарплату) який вони використовують вважається прийнятним. Тепер, після нашого виявлення цього факту, це питання вирішується. Отже, ми розглядаємо це як ненавмисний витік даних. Багато інших інцидентів, ймовірно, виникають через відсутність обізнаності, оскільки це не є системними інцидентами, а особи, що є винуватцями - одиниці. Працівникам відомо, що медичну інформацію та іншу інформацію зі служб соціального обслуговування слід зберігати конфіденційно, і, в основному, це так і відбувається. Здається, що ці інциденти виникають, коли окремі співробітники не розуміють можливих наслідків своїх дій, і тому ми вважаємо їх ненавмисними.

4.2.2 Компанія 2

Тип даних	Політика компанії
Username and Password	Персональні паролі є конфіденційною інформацією, проте нічого не сказано про паролі до спільних аккаунтів

Табл. 9 Аналіз тригерів трафіку та політики компанії(Компанія 2)

Політика компанії не визначає жодного виду даних як конфіденційних, окрім паролів, але залишає це на суд користувача на підставі класифікацій, зазначених у політиці. Серед класифікацій "конфіденційно", "внутрішнє" та "публічне" ми можемо вважати, що ім'я користувача та пароль повинні бути серед перших двох. Це також було виражено під час інтерв'ю. Згідно з нашою концепцією, це може бути або суб'єктивним стандартом, коли дійсно немає іншого способу здійснити цю передачу, і тому вважається прийнятним надсилати ім'я користувача та пароль незашифровано. Або це може бути відсутністю усвідомлення щодо безпеки, коли користувачі насправді не розуміють ризики надсилання імені користувача та пароля без шифрування. Таким чином, в цьому випадку нам справді не відомо, чи навмисний цей витік даних, чи ненавмисний. Ми виконали аналіз трафіку анонімно, тому не можемо запитати користувачів про їхні наміри.

Перехресне порівняння

4.3.1 Інтерв’ю

Питання	Компанія 1	Компанія 2	Різниця
Скільки людей працює у інформаційній безпеці?	Немає призначених персон та ролей	Є одна відповідальна за це людина. Працює вона	Компанія 2 має визначену роль та людину
Хто відповідальний за ISSP?	Немає призначених персон та ролей. Місцева адміністрація вирішує.	IT менеджер	Компанія 2 має відповідальну людину
Як часто оновлюється ISSP?	«на льоту»	«на льоту». Коли потрібно	
Як розповсюджуються знання про ISSP?	Під час періоду адаптаці (при прийомі на роботу). Подальші оновлення - через Інтранет	Під час періоду адаптаці (при прийомі на роботу). Подальші оновлення - через Інтранет. Через систему управлінян документами.	
Як працівники дізнаються про ризики, пов'язаних із витоком даних?	Здоровий глузд та засоби підтримки IT	Під час адаптації. Далі SETA тренінги.	Компанія 2 впроваджує SETA
Як проводяться навчання по зменшенню ризиків?	Засоби підтримки IT	Під час адаптації. Засоби підтримки IT	

Яких регуляторних норм повинна дотримуватись організація?	Законодавство щодо архівування, обробки інформації про пацієнтів та особисто ідентифікованої інформації.		Компанія 1 повинна дотримуватись регуляцій
Чи знаєте ви про випадки витоку даних?	Ні	Ні	
Яким буде наслідок витоку даних?	Розслідування та штрафи	Штрафи, втрата довіри клієнтів, доходу	Компанія має втрату доходів
Які данні ви вважаєте конфіденційними?	Особиста інформація, інформація на медичну тему	Особиста інформація, вихідний код	Майже повністю різні
Як ви дізнаєтесь про випадки витіканян даних?	Усно	Усно	
Які кроки ви приймаєте для покращення культури безпеки?	Робота над загальними культурними рисами у надії, що вони матимуть вплив і на культуру безпеки.	Навчання під час адаптації. Через службу підтримки IT.	Повністю різні
Як ви справляєтесь з інцидентами інсайдерства?	Письмова догана. При повторному інциденті – правові рішення.	Письмова або усна догана. При повторному інциденті – правові	Компанія 2 може звільнити порушника

		рішення та звільнення.	

Табл. 10 Перехресне порівняння інтерв'ю

Ми поставили однакові питання обом компаніям, тому ми маємо можливість порівняти їх відповіді. Компанії зовсім різні: муніципалітет працює над вирішенням справ для покращення громади, тоді як компанія, що розробляє програмне забезпечення, займається розробкою та підтримкою інтелектуальної власності. Ми хотіли побачити, як це відображено в інтерв'ю.

Почнемо з організації забезпечення безпеки. Компанія 1 не має конкретної організації для цього. У компанії 2 це питання вже вирішено.

Щодо Політики забезпечення інформаційної безпеки (ISSP), вони збігаються, за винятком того, що компанія 2 розпочала процес розробки стратегії підвищення обізнаності з питань безпеки. Обидві компанії здійснюють навчання з питань безпеки як частину процесу вступу на роботу, і обидві компанії здійснюють оновлення ISSP за потребою.

На питання щодо впливу витоку даних компанія 2 насправді провела оцінку ризиків, тому вони мають досить добре знання про можливий вплив. Компанія 1 має глибокі знання, але також обмежується штрафами і поганою репутацією.

Питання про типи даних, які є конфіденційними, показує велику різницю. Компанія 1 обробляє особисту ідентифікаційну інформацію та медичну інформацію, тоді як компанія 2 обробляє інформацію про клієнтів та інтелектуальну власність.

Останньою різницею є вплив порушень, де незначні події вирішуються подібно, але в компанії 2 серйозна подія може призвести до звільнення працівника.

4.3.2 Трафік

Тип даних інциденту	Компанія 1	Компанія 2
Номер соц. страхування, зарплатня	9	0
Номер соц. страхування	14	0

Список з більше, ніж 10 номерами страхування	1	0
Username&Password	1	16
Медична інформація	1	0

Табл. 11 Перехнесне порівнянн інцидентів

Компанія 1 та компанія 2 абсолютно різні і обробляють абсолютно різні типи даних. Той факт, що інциденти витоку даних значно відрізняються, не було великим сюрпризом. У компанії 1 приблизно 1800 активних працівників, тому розподіл витоків даних на різні типи також не є сюрпризом. Основна кількість інцидентів від компанії 1 була пов'язана з відділами кадрів та номерами соціального забезпечення.

Компанія 2 мала інциденти лише одного типу - ім'я користувача та пароль, які передавалися зовнішнім партнерам в незахищеному вигляді. Ми були досить приємно здивовані тим, що інтелектуальна власність компанії не була частиною інцидентів.

ВИСНОВКИ

Запобігання витоку даних неможливо, завжди знайдеться хто-небудь, хто зможе обійти перешкоди, які ви створюєте. Вони можуть скопіювати дані на USB-флешку або CD, але ви можете запобігти цьому. Вони можуть роздрукувати дані та винести їх у паперовому вигляді. Або вони можуть зробити фотографії даних за допомогою своїх смартфонів. Ви можете використовувати багато технічних засобів, щоб запобігти цьому, проте це може бути дуже складним завдання. Людській фантазії немає меж, тому ви не зможете передбачити всі навмисній дії щодо витоку даних. Проте, навіть якщо неможливо досягти 100% політики безпеки, ви повинні намагатися наблизитися до цього.

Теорія запланованої поведінки стверджує, що навмисний витік даних ґрунтується на намірі не співпрацювати з ISSP. Ми не змогли знайти жодних теорій про ненавмисний витік даних, але ми базували нашу концепцію на теорії запланованої поведінки і додали недостатню обізнаність як причину ненавмисного витоку даних. Наша теоретична база ґрунтується на тій же теорії, але ми додали інші фактори до поведінки користувача, які призводять до витоку даних, який не є навмисним. Події, які були вчинені незважаючи на положення політики про їх заборону, можуть бути викликані суб'єктивною нормою і, отже, класифікуються як намірений витік даних, оскільки вони не відповідають ISSP. З іншого боку, якщо дія не згадана в політиці, користувач все ще дотримується ISSP. У таких випадках ці події є ненавмисним витоком даних, але користувачі можуть не використовувати здоровий глузд через відсутність обізнаності.

Ми не запитували користувачів про їхні наміри, коли вони виконували дії, що призвели до інциденту. Таким чином, категоризація подій на намірений та ненамірений витік даних базується на порівнянні забраних даних з ISSP. Завжди пам'ятайте, що витік даних залишається витоком даних, незалежно від намірів. Через відсутність коментарів працівників після інцидентів ми не можемо оцінити серйозність порушення. Нехай цим займаються їхні компанії.

Функція DLP (Data Loss Prevention) в брандмауерах Checkpoint - це корисна можливість, яка допомагає запобігти витоку даних. Але вона вимагає багато налаштувань для обмеження кількості помилкових позитивів. Це не штучний інтелект, він просто створює подію, якщо знаходить певний шаблон. Наприклад, під час тестів у компанії №1 ми виявили багато помилкових позитивів через те, що активували одну з найкращих практик відповідно до вимог PCI щодо пін-кодів кредитних карт. Таким чином, кожного разу, коли виявлялися дані, що складалися з чотиризначного числа, брандмауер вважав це пін-кодом і створював подію DLP. Тепер ми розуміємо, що активовувати такий функціонал для всього трафіку є повним безглуздям. Однак для фінансового відділу такий функціонал на обмеженій частині мережі може бути дійсно корисним.

Нині існує БД із багатьма типами даних, визначеними наперед. Проте більшість з них не працюють на українському ринку. Ви дійсно повинні створювати власні типи даних для пошуку та створювати ключові слова для різних частин організації. У випадку №1 ми виявили один інцидент, який мав критичну серйозність. Його не виявлено завдяки ключовим словам, які ми визначили, або типам даних, які ми вказали. DLP-подія була викликана відправленням великого файлу по електронній пошті. Після цього ми перевірили цю подію і зрозуміли, що дані у цьому файлі є справді конфіденційними. Так що виявлення цього інциденту було ділом удачі. Ви повинні розуміти, що впровадження рішення DLP - це не завдання "встановити і забути". Ви повинні постійно вдосконалювати базу даних ключових слів, переконуючись, що ви виявляєте все більше та більше даних, що витікають, і оновлювати її з урахуванням того, які дані додаються до електронних систем організації.

Ще одним висновком є те, що для захисту компанії необхідно виконувати інспекцію SSL. У випадку №1 ми бачили, що приблизно 24,4% трафіку було загальним SSL-трафіком. Крім того, існують різні програми, такі як Dropbox та Facebook, які використовують SSL для захисту трафіку. Таким чином, інспекція SSL є дійсно важливою для DLP. Виконання інспекції SSL не було можливим у тих реалізаціях, які ми тестували, оскільки ми не встановлювали брандмауери в режимі «inline». Вони були встановлені у режимі «tap», тому трафік ззовні існуючого брандмауера був дубльований на встановлений нами брандмауер DLP. У режимі «inline» ви можете ввімкнути інспекцію SSL, яка розшифрує сеанс і встановить новий сеанс для передачі даних до початкового пункту призначення. Роблячи це, SSL-зашифровані дані перехоплюються, розшифровуються, а далі їх можна інспектувати. Але, на наш погляд, це порушує ключову особливість SSL-протоколу, а отже більше неможливо гарантувати автентичність пакетів даних. Таким чином, потрібно приймати рішення, що важливіше: забезпечення цілісності даних кінцевого користувача чи запобігання витоку даних організації?

Ще однією технічною складністю є те, що технологія прикріплення сертифіката стала все більш поширеною для запобігання атакам типу "людина посередині". Це технологія, яка використовується для забезпечення того, що сертифікат клієнта та сертифікат сервера співпадають, і сервер та клієнт виконують подвійні рукостискання для авторизації одне одного. Зробивши це, ви можете гарантувати, що ніхто не змінив сертифікат в процесі передачі між клієнтом і сервером. Це обмежує можливість виконання інспекції SSL, оскільки технологія інспекції SSL ґрунтується саме на цьому. Припиненні SSL-тунелю на середині шляху і створенні нових тунелів.

Важливо зазначити, що ми звернулися до декількох різних організацій і запросили їх взяти участь у цьому дослідженні. Їхня участь могла б надати цьому дослідженню більше даних і точніше відображати реальну ситуацію. Результати також просвітили б організації щодо наявності витоку даних, як вони відбуваються та як компаніх справляються в плані боротьби з витоком даних порівняно з іншими організаціями, що беруть участь у дослідженні. Оскільки це дослідження взаємодіє з конфіденційною інформацією, яка має залишатися конфіденційною від інших організацій та несанкціонованих осіб, ми були готові укласти угоду про нерозголошення і зберігати анонімність організацій. У кінці кінців у дослідженні взяли участь лише дві організації, оскільки інші відмовилися від пропозиції про участь у дослідженні через питання щодо безпеки. Навіть якщо більшість організацій відмовилися брати участь у дослідженні, можна припустити, що вони турбуються про витік даних і не хочуть, щоб несанкціоновані особи мали можливість досліджувати їхню мережу та безпеку. По спілкуванню з організаціями, які взяли участь у дослідженні, вони пояснили, що це дослідження допоможе їм в покращенні безпеки та мінімізації можливого витоку даних у майбутньому. Вони сказали, що не розуміють, чому більшість організацій відмовилися від пропозиції виявити витоки даних в своїй організації безкоштовно. Одна з організацій навіть попросила нас виконати ті ж завдання, як у цьому дослідженні, але в більшому масштабі і також покращити їхню безпеку від витоку даних. Це свідчить про те, що організації турбуються про витік даних, які відбуваються у їхній організації, і вони хочуть нашої допомоги, що підтверджує, що це дослідження відповідало їх очікуванням.

Також коли мирозглядали ISSP компаній, то виявили, що вони не дотримуються жодних стандартів. Існують кілька стандартів, які можна використовувати для створення ISSP, одним з них є ISO 27002. Через те, що ISO 27002 - це платний стандарт, компанії віддають перевагу створенню власної політики з нуля, і, як ми бачили, вони пропускають деякі важливі аспекти та роблять інформацію та точки прийняття рішень зайвими і важкими для оновлення та перевірки.

ISSP Компанії 1 загалом є дуже відкритою політикою. Практично дозволяється все, якщо співробітник може показати, що те, що він робить, пов'язано з роботою. Щодо політики також відсутні інструкції стосовно запобігання саботажу та порушень. У ній не сказано нічого про антивіруси, шифрування даних, системні послуги, контроль доступу або віддалених працівників. І в цьому контексті ми вважаємо дивним те, що Угода про нерозголошення не охоплює всю конфіденційну інформацію у всіх підрозділах, а лише особисто ідентифіковану інформацію в галузях соціального захисту та освітніх послуг.

Ми можемо сказати, що політика від Компанії 2 є обширною і охоплює багато аспектів. Однак є питання, що багато положень в політиці є зайвими, одна і та ж інформація перерахована в кількох місцях. За копіями політик, які ми отримали, вони всі послідовні, проте є проблема, яка полягає в тому, що якщо вам хочеться щось змінити, то доведеться оновити інформацію в кількох місцях. Досить багато інформації також було застарілою, посилаючись на системи або функції, які вже не були актуальними. Нові системи не згадані взагалі. Ми також виявили, що в різних розділах не вказані деякі деталі: наприклад нічого не сказано про зберігання конфіденційних даних в хмарному сховищі, або про те, як забезпечити безпеку даних під час обробки. Класифікація даних, на наш погляд, покладена на користувача самостійно, і в політиці не сказано нічого про те, як обробляти дані клієнтів.

Результати наших виявлень показують, що основною причиною ненавмисного витоку даних є невиконання співробітником процедур та політики. Існує багато причин такої поведінки. Можливо, процедури не відповідають завданню, яке вони виконують, можливо, відсутні технічні системи або вони працюють неналежним чином, або, можливо, працівник не знає, як виконувати завдання. За результатами інцидентів, які ми виявили в компаніях, ми вважаємо, що основною причиною є відсутність усвідомленості та обізнаності. Під час цієї дипломної роботи ми створили теоретичну модель на основі теорії запланованої поведінки. Теорія запланованої поведінки вказує, що самоефективність, суб'єктивні норми та ставлення - це теми, які призводять до навмисного витоку даних. Для покриття ненавмисного витоку даних ми додали до нашої теорії тему усвідомленості та обізнаності у питаннях безпеки як причини ненавмисного витоку даних. Для детальнішого розгляду, ненавмисний витік даних відбувається через відсутність навчання з питань безпеки, освіти з питань безпеки та усвідомленості безпеки. Результати наших досліджень повністю відповідають цій теорії.

Йдучи далі, що б ми могли зробити для зменшення витоку даних? У ідеальному світі у вас була б велика культура безпеки, яка б вирішувала дане питання. Культура безпеки - це ключ до успіху. Проте створення культури безпеки складне завдання, воно вимагає часу, і ви ніколи не зможете залучити всіх співробітників до цієї культури. Люди різні і мають різні погляди на різні питання. Створення цієї культури включає багато аспектів, таких як навчання з питань безпеки, підготовка та усвідомленість, але це не обмежено лише цими аспектами.

Ще однією проблемою є те, що більшість компаній сьогодні не мають видимості щодо даних, які покидають територію компанії. Ви не можете захистити те, про що не знаєте. Це можна вирішити, встановивши механізм

виявлення витоку даних (DLP). Це буде менш нав'язливим, оскільки воно не перешкоджатиме транзиту даних, а ви отримаєте добру перспективу, куди вам потрібно зосередити свої ресурси. Впровадження рішення з захисту витоку даних не так просто, як здається. Дійсно потрібно багато налаштувань, щоб змусити його відловлювати те, що вам потрібно. Якщо ви отримуєте занадто багато помилкових сигналів, буде важко визначити, що є справжнім інцидентом. Ми бачили це під час дослідження в Компанії 1, оскільки ми додали до DLP пошук відповідності PCI і, отже, пошук PIN-коду, ми отримали практично 300 000 помилкових сигналів. Знайти 32 справжні інциденти було схожим на пошук голки в купі соломи. Ми також виявили кілька інцидентів на чистому везінні, адже DLP не включав жодних ключових слів для інцидентів, але з іншого боку, він спричинив подію через передачу великих файлів. Так що налаштування ключових слів - це ключ до працюючого рішення DLP, і це повинно бути постійною задачею. Впровадження рішення з безпеки не повинно бути завданням "встановити і забути".

Отже, наблажажмось до вхідних даних для налаштування DLP. Якщо б ми фокусувалися лише на виконанні ISSP цих компаній, у нас не було б багато інцидентів. Причиною цього було те, що в ISSP бракувало багато інформації. За результатами, які були нам представлені, ми можемо сказати, що вони не охоплюють все, що повинно бути включено. Наша рекомендація полягає в тому, щоб базувати ISSP на якомусь стандарті. Наприклад в цьому дослідженні ми базувались ISSP з ISO 27002:2022, що надає вам хорошу базу при створенні політики. Компанії, що взяли участь у дослідженні, створили свої власні політики з нуля, і це випадок багатьох компаній сьогодні. Ризик полягає в тому, що ви можливо пропустите щось і створите політику, яка не охоплює всі необхідні області. Ще однією проблемою було те, що політики були застарілими. Тому ми рекомендуємо впровадження процедури управління життєвим циклом політики безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

otecting organizational competitive advantage: A knowledge leakage perspective. Computers & Security, 42, 27–39.

3. Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes 1991;50(2):179-211

U
R
L
:

rd a unifying theory of behavioral change. Psychological Review 1977;84(2):191-215.

6. Bandura, A. (1991). Social cognitive theory of self-regulation. Organizational Behavior and Human Decision Processes 1991; 50:248-87.

(дата звернення: 22.04.2023).

U
R
L
:

U
R
L
:

10. Brendan, O. (2014). Whoops! how your “convenience” broadcast your secrets.
(дата звернення: 15.04.2023).

(дата звернення: 03.04.2023).

u, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly 2010;34(3):523-48

ions’ Information Security Policy Compliance: Stick or Carrot Approach? Journal of Management Information Systems, 29(3), 157–188.

13. Colwill, C. (2009). Human factors in information security: The insider threat –

s
e
c
u
r
i
t
y

16. D’Arcy, J., Hovav, A. & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research, 20(1), 79–98.

U
R
L
:
h
t
t
p
s
:
/
/

19. Goel, S., & Shawky, H. (2009). Estimating the market impact of security breach announcements on firm values. Information and Management, 46, 404–410.

Protection motivation and deterrence: a framework for security policy compliance in organizations. European Journal of Information Systems 2009;18(2):106-25.

stems. Communications of the ACM 2005; 48(8):72-7.

:

: веб-сайт. URL:
:
звернення: 20.06.2023).

в
.
е
б
в
е
с
б
а
й
т
а
U
й
R
т
L
U
R
L
(
д
а
т
а

з
в
е
р
н
е
н
н
я

(дата звернення: 10.05.2023).