МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ПРИСТУПА ДЕНИС ВІТАЛІЙОВИЧ

Допускається до захисту:
Завідувач кафедри
інформаційних технологій,
д.т.н., доцент, Нескородєва Т. В.
«__»_____20__р.

МЕТОДИ ПРОТИДІЇ ФІШИНГОВИМ АТАКАМ, ЛЮДСЬКИЙ ВИМІР

Спеціальність 125 Кібербезпека
Кваліфікаційна (бакалаврська) робота

Науковий керівник:
Крижановський В.Г,
професор кафедри
інформаційних технологій,
д.т.н., професор

_____
(підпис)

Оцінка : _____ / _____ / _____
(бали/за шкалою ЄКТС/за національною шкалою)

Голова ЕК: _____
(підпис)

Вінниця – 2022

АНОТАЦІЯ

Приступа Д. В. Методи протидії фішінговим атакам, людський вимір. Спеціальність 125 “Кібербезпека”. Донецький національний університет імені Василя Стуса. Вінниця. 2022 рік.

У кваліфікаційній роботі проаналізовано тенденції розвитку протидії фішингу та політики інформаційної безпеки компанії. Запропоновано модульну політику компанії протидії фішингу.

Ключові слова: Фішинг, протидія фішингу, політики інформаційної безпеки.

26 сторінок, 2 рисунків, 11 джерела.

ABSTRACT

Prystupa D.V. Methods of counteracting phishing attacks, the human dimension. Specialty 125 "Cybersecurity". Vasyl Stus Donetsk National University. Vinnitsa. 2022.

The qualification work analyzes the trends in the development of anti-phishing and information security policy of the company. A modular anti-phishing policy has been proposed.

Keywords: Phishing, anti-phishing, information security policies.

26 pages, 2 figures, 11 items.

ЗМІСТ

ВСТУП

Інтернет мережа щільно інтегрувалась в наше життя. Люди все більше використовують її для роботи, відпочинку, шопінгу та іншого.

Люди повністю поглинули в використання інформаційної мережі інтернет. Відповідно збільшилось популярність фішингу тобто шахрайства метою якого є несанкціонований доступ до конфіденційної інформації користувачів.

В даній роботі ми зосередимось на захисті інформації працівників від фішингу.

Потрібно розуміти що який би не був захист від шахрайства він не дає стовідсоткового гаранту захисту, але вона збільшує рівень захисту компанії.

Короткі відомості

В даній роботі буде розглянутий яким чином можна побудувати політику для захисту працівників та програмні рішення які удосконалять систему протидії фішингу які потрібно впровадити для захисту співробітників.

В роботі будемо розглядати як основний метод дії зловмисника комп’ютер та людину на основі яких і буде побудована модульна політика компанії для захисту від фішингу.

Де буде здійснюватися захист від фішингу.

Для побудови ефективної модульної політики компанії протидії фішингу, потрібне розуміння на якому аспекті буде будуватись захист та принципи на яких будуватимуть політику, яка буде відповідати необхідним нам потребам.

Потрібно розуміти що зазвичай персональний комп’ютер і так достатньо захищений і основні загрози лунають від користувача тому головний аспект політики буде зроблений на користувачі в другу чергу буде персональний комп’ютер на програмному рівні.

Захист буде відбуватись на тих аспектах, де працівник безпосередньо можу зустрітись з фішингом.

РОЗДІЛ 1 було проаналізовано що відбувається у теперішньому світі з питання фішингових атак та кіберзлочинності.

Було проведені обстеження сучасних методів протидії кіберзлочинності та аналіз сучасних політик інформаційної безпеки та були проведено аналіз щодо виявлення їх сильних та слабких сторін.

Після цього було надане обґрунтування створення модульної політики безпеки протидії фішингу для посилення ефективності роботи існуючих методів протидії фішингу.

РОЗДІЛ 2 для зменшення успіху випадків фішингу у компанії було розроблена модульна політика компанії для забезпечення безпеки роботи компанії.

РОЗДІЛ 3. Створено документу модульної політики безпеки заради протидії фішингу.

РОЗДІЛ 1 ТЕНДЕНЦІЇ РОЗВИТКУ ПРОТИДІЇ ФІШИНГ АТАКАМ ТА РОЗВИТОК ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Актуальність обраної теми в сучасних реаліях

Актуальність роботи зумовлена все більшим розвитком інтернет-технологій, та активним проведенням інформаційної війни і не тільки з країною агресором та збільшенням популярності фішингу тобто шахрайством метою якого є несанкціонованим доступом до конфіденційної інформації.

Фішинг – це дія зловмисників через мережу інтернет з метою отримання несанкціонованого доступу до даних користувача\працівника. Це одна з найпопулярніших методика злочинів у мережі інтернет.

За звітом Phishlabs [2] було виявлено основні тенденції за 2021 рік що до зростання фішингу в порівняні з 2020 роком він виріс на 32 % Вішинг інциденти з 2020 до 2021 зросли у двічі. У соц-мережах загроза зросла на 82%

З початку 2021 року за опитуванням в ОЛХ [2] [4] :

- 45 % опитаних хоч раз зустрічались з фішингом. У 2020 році цей відсоток досягав 22 %
- 2/3 випадків на користувачів з міста.
- 60% жінок 40% чоловіків. Такий відсоток серед статі.
- 14 % атакованих втратили свої кошти.
- 83% атак через стороні посилання на інші ресурси та соц-мережі.
- 6% через СМС повідомлення.

Ця статистика демонструє критичність цієї проблеми

Фішинг буває кількох видів: [3]

- СМС-фішинг, фішинг коли жертва отримує повідомлення на мобільний телефон.
- Інтернет-фішинг, зловмисник відправляє повідомлення на персональний комп’ютер або створює фішинговий сайт
- Вішинг – під час телефонного дзвінку вимагає дані кредитних карток тощо.
- Шкідливе програмне забезпечення – створення програм які розсилаються поштою щоб коли їх відкрили вони вкрали дані користувача.

1.2 Дослідження тенденцій з питання методів протидії фішингу.

Цілю більшості атак фішерів зосереджений на людині. В більшості випадків не підготовлений користувач не відрізнить фішинг лист від звичайного

Розглянемо основні методи розпізнавання фішинг листів які вже існують:[6]

Відповідно до цієї статі є 2 основні методи розпізнавання фішинг листів і сайтів:

1) Підготовка працівників та користувачів за рахунок поглиблення їхніх знань в області природи фішингу заради збільшення шансу розпізнавання працівником фішинг листів та сайтів.
2) При допомозі програмних та апаратних засобів. Він виключає шанс на людський фактор та набагато дешевший у випадку впровадження адже людей навчити набагато важче ніж спеціалізований для цього програмний засіб.

Він включає в себе:

-Чорний та білий лист сайтів для роботи.

- Евристику тобто набір характеристик в фішинг атаках.

- Візуальна схожість.

Що перший що другий метод має велику кількість недоліків. Але кожен метод можна покращити. Наприклад людину можна навчити за допомогою зовнішніх та внутрішніх курсів. Програмний засіб можна поліпшити роботу аналізатора за допомогою машинного навчання. Але найкращий захист це комбінований. Також не потрібно забувати, що ці методи дієві лише тоді коли фішинг був виявлений.

Тому важливо прорахувати та побудувати політику компанії заради комплексного захисту компанії.

1.3 Дослідження тенденцій з побудови політики інформаційної безпеки

Почнем з того що політика інформаційної безпеки це правила, вимоги, обмеження що до дій працівника та в цілому регламент дій компанії під час критичної ситуації що до збільшення інформаційної безпеки компанії.

Згідно дослідження Deloitte в 2006 році. Статистика демонструє, що в компанії з політикою інформаційної безпеки шанс злому зменшився в порівняні з компанією в якої політика відсутня. [7]

Кожна політика інформаційної безпеки базується на головному стандарті ISO/IEC 27001:2013 суто його полягає в постійному покращені політики інформаційної безпеки та регламентує як оцінювати, ліквідувати що до потреб компанії. Вимоги, викладені в ISO/IEC 27001:2013,цей документ є спільним і застосовується до усіх видів організацій. [8][9]

Розглянемо приклад вже побудованої політики інформаційної безпеки: [10] [11]

Політика інформаційної безпеки АКЦІОНЕРНОГО ТОВАРИСТВА «ТАСКОМБАНК»

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПАТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК»

Що у першому що у другому прикладі сфера застосування розповсюджується на увесь банк, це зменшує можливість конкретним відділам негайно реагувати на непередбачені інциденти, змінювати свою політику міняти програмне та апаратно-програмне забезпечення.

Також в цих політиках інформаційної безпеки передбачений перегляду документа а не удосконалення його під час всього часу роботи, що робить його не працездатним в момент коли з'являється нова вразливість яка не передбачена за довгий час.

1.4 Визначення напрямків роботи зі створення модульної системи протидії фішингу.

З огляду на вище викладені фактори ми можемо визначити та сформулювати основні проблеми та недоліки політики інформаційної безпеки компанії та плюси впровадження модульної політики інформаційної безпеки.

Основною проблемою є дія цього документу на усю компанію. Для великих компаній цей документ підходить, але для середніх і малих краще використати модульну систему.

Модульна політика інформаційної безпеки полягає в тому що модульність передбачає використання правил з неї в не усіх сегментах компанії разом, її можна поєднувати з повноцінною політикою інформаційної безпеки компанії. Що дає змогу бистрої заміни правил у цьому сегменті.

Також можливо використання цієї політики як конструктор у який компанії добавляють та забирають не потрібні сегменти відповідно до потреб компанії. Це може пригодитись новим компаніям які тільки почали створювати свою політику інформаційної безпеки і щоб закрити якусь не досконалість нової політики використовувати модульну політику інформаційної безпеки.

Тобто суть цієї політики вирішити нагальну проблему, з подальшою заміною на повноцінну політику. Це пов'язано з довгим часом розробки повноцінної політики і підготовкою її під потреби компанії.

Проблема полягає в тому коли компанія тільки заснувалась неможливо створити ідеальну політику яка піді йде у всіх випадках.

В таких моментах я пропоную використовувати модульну політику інформаційної безпеки, вона буде стосуватись якогось одного сегменту випадків. Її можна використовувати в екстрені моменти. За нею повинен дивитись один спеціаліст який буде лише над нею і працювати, наробітки з неї можна використати і в основній політиці.

Таким чином в результаті пошуку тенденцій й проблематики в питаннях протидії фішингу ми можемо стверджувати, що основними напрямками роботи є

1)Створення політики протидії фішингу

2)Рекомендації коли варто використовувати політику.

Проблематику людського виміру відобразив якісно новий підхід до розробки політики інформаційної безпеки, у якій людина грає нову роль як суб’єкта та об’єкта. Суть якого полягає у визнані людини як головного фактору безпеки усіх і це визначає безпеку компанії.

1.5 Висновок РОЗДІЛ 1

Отже ми проаналізувати стан справ з протидії фішингу. Розібрали основні методики фішингу, тенденції з протидії фішингу та важливість впровадження політики інформаційної безпеки компанії. А саме модульної версії. Також ми розібрали основну проблематику звичайної політики та модульної у яких випадках вона підходить.

2. ВИМОГИ ДЛЯ СТВОРЕННЯ ПОЛІТИКИ ПРОТИДІЇ ФІШИНГУ

2.1 Вимоги до побудування політики компанії для протидії фішингу.

Оскільки розроблювана політика є для компанії і призначена для використання групою людей в потрібно її розбити на 4 основні етапи протидії на яких буде створений захист:

1. Збільшення складності до користувацьких акаунтів та робочих машин вашої компанії
2. Бистре реагування та повідомлення користувачам на вже отримані фішингові листи
3. Створення захисту проти не виявлених фішингових листів
4. Бистре реагування на успішний фішинг та вжиття заходів заради ліквідації

Рис 2.1 – Блок схема послідовності розробки модульної політики протидії фішингу по аспектам.

Ми будем робити аспект на рекомендаціях що до впровадження та навчання наших співробітників. Але не варто забувати про використання апаратно програмне забезпечення та програмне забезпечення для впровадження у вашу компанію. Це збільшить захищеність компанії та допоможе зменшити вплив людського фактору на організацію.

Основні вимоги до апаратно програмного забезпечення та програмного забезпечення:

1. Захист на випадки в реальному часі
2. Захист у хмарних технологіях
3. Захист від підроблених повідомлень
4. Безвідмовність
5. Простота налаштування

2.2 Розробка політики компанії для роботи з користувачами для протидії фішингу.

На кожному із 4 етапів ми створеному правила так щоб на кожному етапі організувати свою роботу з іншими членами компанії щоб ефективно працювала система безпеки.

1) Збільшення складності до користувацьких акаунтів та робочих машин вашої компанії:

1.1 Скорочення доступності інформації якою може скористатись зловмисник при отримані доступу до пошти за допомогою рекомендацій NCSC

1.2 Запровадження DMARC системи суть якої полягає в перевірці повідомлення тобто чи є автор цього повідомлення реальною організацією.

1.3 Запровадження SPF політики відправника.

1.4 Впровадження технології протидії фішингу та спаму для виявлення легітимної пошти DKIM

1.5 Перегляд інформації яка розміщена на сайті компанії та соц-мережах. Та видалення інформації якою може використати зловмисник.

1.6 Створення переліку інформації яку можуть викласти ваші партнери.

1.7 Проведення тренінгів з працівниками для їх розуміння яку інформацію вони можуть викладати у соц-мережах.

1.8 Регулярна перевірка пошти на вміст фішингу адміністраторами компанії.

1.9 Налаштування DMARC з політикою карантину, для повторної перевірки адміністратором.

1.10 Перевірка відповідності хмарної електронної пошти на фільтрацію, щоб не блокувались робочі файли.

1.11 Заборона власноруч працівникам відкривати повідомлення які не пройшли фільтрацію

2) Бистре реагування та повідомлення користувачам на вже отримані фішингові листи

2.1 Пояснення працівникам компанії як реагувати на підозрілий лист і в які моменти звертатись до адміністратора за подальшими діями.

2.2 Перевірка користувачів на відповідальність що до фішинг загрози

2.3 Пояснення працівникам основні риси фішинг повідомлень. Впровадження CPNI рекомендацій для цього.

2.4 Проведення регулярних тренінгів з працівниками для розуміння будови фішинг листів.

2.5 Побудова пріоритетів підготовки працівників з різних відділів по зацікавленості зловмисників.

2.6 Робота з працівниками таким чином, щоб це не порушувало їх права.

2.7 Ознайомлення працівників з звичайними процесами вашої компанії, щоб при виникненні незвичайного запиту користувач розумів що потрібно звернутись до користувача.

2.8 В компанії потрібно дублювати важливі повідомлення іншим методом зв’язку.

2.9 Розробка зовнішнього виду повідомлень у роботі між користувачами.

2.10 Поясніть вашим партнерам та працівникам яку інформацію вони можуть надати та запросити у інших компаній, клієнтів.

2.11 Розробка процесу ефективної подачі звітів адміністратору.

2.12 Адміністратори повинні вести зворотній зв'язок з працівниками

2.13 Впровадьте альтернативний метод зв’язку від працівника до адміністратора.

3) Створення захисту проти не виявлених фішингових листів

3.1 Вчасне оновлення програмного забезпечення адміністраторами.

3.2 Заборона працівникам встановлення власного програмного забезпечення

3.3 Надання дозволів на певні дії які не пов’язані з звичайною роботою працівника

3.4 Встановлення проксі серверів

3.5 Використання DNS державного сектору (за можливості)

3.6 Введення двох факторної аутентифікації на робочі пристрої та пошту

3.7 Введення програмного забезпечення для паролів Keypass

3.8 Використання біометричних даних та або флеш ключ для входу до системи.

3.9 Права адміністратора надаються лише за потреби і на короткий час.

3.10 Видалення користувачів які більше не працюють в компанії.

4) Бистре реагування на успішний фішинг та вжиття заходів заради ліквідації

4.1 Створення запасних методів зв’язку з адміністратором в екстрений момент.

4.2 Адміністратори повинні увесь робочий час монітори ситуацію для виявлення загроз.

4.3 Впровадження хмарного монітору випадків.

4.4 Підготовка організації до кроків які потрібно зробити під час інциденту.

4.5 Створення плану дій який буде відповідати законодавчій політиці країни.

4.6 Попереднє тестування плану екстреної дії перед загрозою.

4.7 Постійне вдосконалення плану що до нових вимог.

2.3 Правила коли застосовується дана політика.

Отже дану політику вводять лише в таких випадках:

- Створення нової повноцінної політики інформаційної безпеки ще не виконана повному обсязі. Коли компанія тільки запроваджує і розробляє політику інформаційної безпеки.
- Негайні проблеми які може закрити модульна політика інформаційної безпеки. Коли трапляється випадок непередбачений основною політикою інформаційної безпеки
- Використання у певних відділах компанії, для зменшення обмеження вільності працівників які цього потребують у деяких випадках.
- Впровадження повної модульності політики заради зменшення бюрократії для оновлення її.

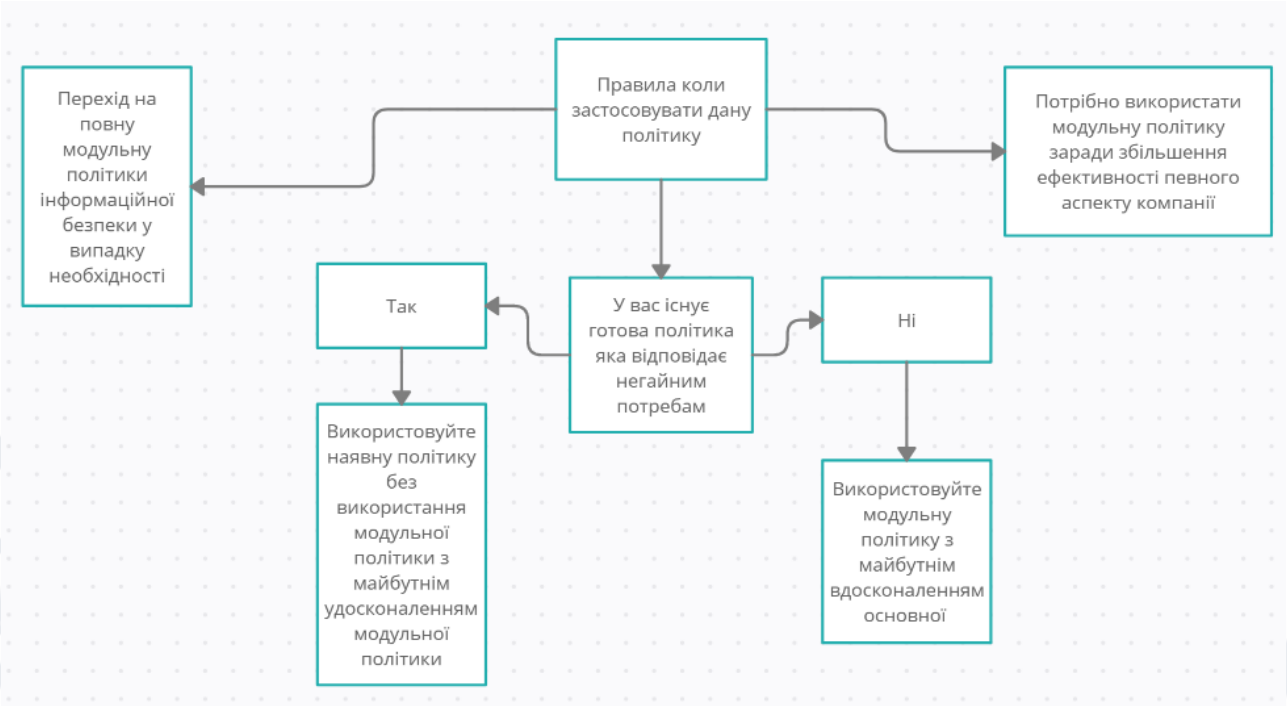

Схема 2.2 Моменти для застосування модульної політики інформаційної безпеки.

Отже з підсумків 2 розділу ми можемо зробити висновок, що є багато випадків коли політика інформаційної безпеки зв'язує руки співробітникам особливо у випадках протидії фішингу. Тому варто розглянути метод модульної інформаційної безпеки компанії, для покращення роботи компанії.

Дану методику побудови можна використовувати і на інші аспекти інформаційної безпеки компанії.

РОЗДІЛ 3 ДОКУМЕНТ МОДУЛЬНОЇ ПОЛІТИКИ ІНФОРМАЦІЙОЇ БЕЗПЕКИ ПРОТИДІЯ ФІШИНГОВИМ АТАКАМ

3.1 Побудова політики інформаційної безпеки протидії фішинговим атакам.

У цьому розділі я розберу поетапно принцип побудови політики інформаційної безпеки.

Даний документ я побудував на основі вже наявних політик інформаційної безпеки, але з використанням правил які запропонував я і з використанням модульної структури яку я запропонував раніше.

Побудова по розділам складається з

1.ВСТУП – на яких стандартах та вимогах була побудована політика.

2.ЦІЛЬ ДОКУМЕНТУ – основні вимоги до політики тобто, принципи яким вона повинна відповідати.

3.ПОЛЕ ЗАСТУСУВАННЯ – вказується місце де діє цей документ.

4. ПРИНЦИП ТА ВИМОГИ ІНФОРМАЦІЙОНЇ БЕЗПЕКИ – основні правила які потрібно впровадити.

5. ПІДХОДИ ЩО ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ – дії персоналу як поводитись з цим документом та відповідальність за роботу з ним.

6.ЗВІТНІСТЬ – час коли повинен проводитись звіт що до роботи політики

7.ПЕРЕГЛЯД ДОКУМЕНТА – час з яким потрібно переглядати документ щодо внесення змін.

На даний момент цей документ ще не ідеальний і він потребує доопрацювання. Але як початковий етап для розробки модульної політики інформаційної безпеки він працюватиме.

ВИСНОВКИ

В роботі було:

1. Вказано що головна суть інформаційної безпеки компанії є політика і чому варто використовувати модульну політику інформаційної безпеки.
2. Побудовані правила у яких випадках модульна політика найбільш дієва
3. Створений документ політики інформаційної безпеки компанії який звертає свою увагу на протидія фішинговим атакам.

Список використаних джерел

1) QUARTERLY THREAT TRENDS & INTELLIGENCE REPORT NOVEMBER 2021. Режим доступу до ресурсу: https://info.phishlabs.com/hubfs/PhishLabs%20-%20QTTI%20Report%20-%20November%202021

2) СТАТИСТИКА ФІШИНГОВИХ ІНЦИДЕНТІВ В УКРАЇНІ ЗА 2021 РІК С.А. Думчиков В.В. Лукічов. Режим доступу до ресурсу: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/34523/91970.pdf?sequence=2&isAllowed=y

3) Кіберзлочинність в Україні Ера цифрових технологій – ера нових злочинів. – Режим доступу до ресурсу: https://uz.ligazakon.ua/ua/magazine_article/EA013606

4) Українці почали вдвічі частіше стикатися з шахраями в інтернеті, найбільше – в месенджерах: результати опитування– Режим доступу до ресурсу: https://blog.olx.ua/26779/ukrainci-stali-vdvichi-chastishe-stikatisya-z-shaxrayami-v-interneti-najbilshe-v-mesendzherax-rezultati-opituvannya

5) Організація протидії кібершахрайству, що використовує фішингові Гончарова Данила Олеговича – Режим доступу до ресурсу: http://ir.nmu.org.ua/bitstream/handle/123456789/154337/%D0%93%D0%BE%D0%BD%D1%87%D0%B0%D1%80%D0%BE%D0%B2.pdf?sequence=1&isAllowed=y

6) Розпізнавання фішингових сайтів з використанням методів машинного навчання Тернопільська Світлана Олександрівна – Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/31430/1/Ternopolska_bakalavr.pdf%D1%84%D1%96%D1%88%D0%B8%D0%BD%D0%B3%D1%83-0c7ea947-ba98-3bd9-7184-430e1f860a44

7)Політика інформаційної безпеки – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%96%D1%82%D0%B8%D0%BA%D0%B0_%D1%96%D0%BD%D1%84%D0%BE%D1

%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8

8) ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements – Режим доступу до ресурсу: https://www.iso.org/standard/54534.html

9) ISO/IEC 27001:2013 – Режим доступу до ресурсу: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

10) Політика інформаційної безпеки АКЦІОНЕРНОГО ТОВАРИСТВА «ТАСКОМБАНК» – Режим доступу до ресурсу: https://tascombank.ua/files/Polityka_IB_2021.pdf

11) ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПАТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК» – Режим доступу до ресурсу: https://www.pinbank.ua/wp-content/uploads/2017/02/Polityka_IB_2016_2.0_2_KT-1.pdf

ДОДАТОК ДОКУМЕНТ ПОЛІТИКИ ПРОТИДІЇ ФІШИГУ

ЗМІСТ

1.ВСТУП

1.1 Політика інформаційної безпеки розроблена відповідно до вимог ДСТУ та чинного законодавства України

●ДСТУ ISO/IEC 27001:2015 «Інформаційні технології Методи захисту. Системи управління інформаційною безпекою. Вимоги”;

● ДСТУ ISO/IEC 27002:2015 “Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки”;

1.2 Політика інформаційної безпеки є документом верхнього рівня у системі управління інформаційною безпекою у моменти негайного випадку.

2.ЦІЛЬ ДОКУМЕНТА

2.1 Мета модульної політики протидії фішингу є бистре та ефективне реагування на випадки інформаційної безпекою в негайні моменти та екстрені ситуації які не передбачає політика інформаційної безпеки, яка забезпечує:

- Захист інформаційних ресурсів компанії пов’язаних з потенційним зовнішніх та внутрішніх загроз пов’язаними з діями працівників і зловмисників.
- Безперервна робота компанії.
- Зменшення ризиків діяльності компанії.

3.СФЕРА ЗАСТОСУВАННЯ

3.1 Дія політики розповсюджується на окремий сегмент захисту проти фішингових атак в негайні моменти.

4 ПРИНЦИП ТА ВИМОГИ ІНФОРМАЦІЙОНЇ БЕЗПЕКИ

Головним принципом є підтримання належного захисту інформаційної системи адміністратором та іншими повноважними членами компанії відповідно цим правилам.

1) Збільшення складності до користувацьких акаунтів та робочих машин вашої компанії:

1.1 Скорочення доступності інформації якою може скористатись зловмисник при отримані доступу до пошти за допомогою рекомендацій NCSC

1.2 Запровадження DMARC системи суть якої полягає в перевірці повідомлення тобто чи є автор цього повідомлення реальною організацією.

1.3 Запровадження SPF політики відправника.

1.4 Впровадження технології протидії фішингу та спаму для виявлення легітимної пошти DKIM

1.5 Перегляд інформації яка розміщена на сайті компанії та соц-мережах. Та видалення інформації якою може використати зловмисник.

1.6 Створення переліку інформації яку можуть викласти ваші партнери.

1.7 Проведення тренінгів з працівниками для їх розуміння яку інформацію вони можуть викладати у соц-мережах.

1.8 Регулярна перевірка поошти на вміст фішингу адміністраторами компанії.

1.9 Налаштування DMARC з політикою карантину, для повторної перевірки адміністратором.

1.10 Перевірка відповідності хмарної електронної пошти на фільтрацію, щоб не блокувались робочі файли.

1.11 Заборона власноруч працівникам відкривати повідомлення які не пройшли фільтрацію

2)Бистре реагування та повідомлення користувачам на вже отримані фішингові листи

2.1 Пояснення працівникам компанії як реагувати на підозрілий лист і в які моменти звертатись до адміністратора за подальшими діями.

2.2 Перевірка користувачів на відповідальність що до фішинг загрози

2.3 Пояснення працівникам основні риси фішинг повідомлень. Впровадження CPNI рекомендацій для цього.

2.4 Проведення регулярних тренінгів з працівниками для розуміння будови фішинг листів.

2.5 Побудова пріоритетів підготовки працівників з різних відділів по зацікавленості зловмисників.

2.6 Робота з працівниками таким чином, щоб це не порушувало їх права.

2.7 Ознайомлення працівників з звичайними процесами вашої компанії, щоб при виникненні незвичайного запиту користувач розумів що потрібно звернутись до користувача.

2.8 В компанії потрібно дублювати важливі повідомлення іншим методом зв’язку.

2.9 Розробка зовнішнього виду повідомлень у роботі між користувачами.

2.10 Поясніть вашим партнерам та працівникам яку інформацію вони можуть надати та запросити у інших компаній, клієнтів.

2.11 Розробка процесу ефективної подачі звітів адміністратору.

2.12 Адміністратори повинні вести зворотній зв'язок з працівниками

2.13 Впровадьте альтернативний метод зв’язку від працівника до адміністратора.

3) Створення захисту проти не виявлених фішингових листів

3.1 Вчасне оновлення програмного забезпечення адміністраторами.

3.2 Заборона працівникам встановлення власного програмного забезпечення

3.3 Надання дозволів на певні дії які не пов’язані з звичайною роботою працівника

3.4 Встановлення проксі серверів

3.5 Використання DNS державного сектору (за можливості)

3.6 Введення двох факторної аутентифікації на робочі пристрої та пошту

3.7 Введення програмного забезпечення для паролів Keypass

3.8 Використання біометричних даних та або флеш ключ для входу до системи.

3.9 Права адміністратора надаються лише за потреби і на короткий час.

3.10 Видалення користувачів які більше не працюють в компанії.

4) Бистре реагування на успішний фішинг та вжиття заходів заради ліквідації

4.1 Створення запасних методів зв'язку з адміністратором в екстрений момент.

4.2 Адміністратори повинні увесь робочий час монітори ситуацію для виявлення загроз.

4.3 Впровадження хмарного монітору випадків.

4.4 Підготовка організації до кроків які потрібно зробити під час інциденту.

4.5 Створення плану дій який буде відповідати законодавчій політиці країни.

4.6 Попереднє тестування плану екстреної дії перед загрозою.

4.7 Постійне вдосконалення плану що до нових вимог.

5. ПІДХОДИ ЩО ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

5.1 Під час введення цієї політики адміністратори переключаються на негайну проблему та вирішують її командою.

5.2 Керівництво підтверджує застосування цієї політики за потреби.

5.3 Відповідальність за адміністраторів бере на себе голова відділу інформаційної безпеки, він вирішує як боротися з проблемою та як покращити політику інформаційної безпеки.

6. ЗВІТНІСТЬ

6.1Надання з оцінки впливу інформаційних систем компанії кожного місяця.

6.2 Звітність щодо впровадження системи управління інформаційною безпекою, моніторингу випадків, рекомендацій що до змін в правилах, реагування на випадки. Відбувається`я раз у місяць або за появи проблеми.

7 ПЕРЕГЛЯД ДОКУМЕНТА

7.1 Політика затверджується Керівництвом

7.2 Політика підтримується в актуальному стані та вносяться зміни за негайної потреби.