НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

До захисту допущено:
Завідувач кафедри
_____ Леонід УРИВСЬКИЙ
«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра
за освітньо-професійною програмою «Телекомунікаційні системи та мережі»
спеціальності 172 «Телекомунікації та радіотехніка»
на тему: «Застосування засобів протидії кіберзлочинності в телекомунікаційних мережах»

Виконав:
студент IV курсу, групи ТС-71
Вайлупов Владислав Олексійович _____

Керівник:
Доцент кафедри ТС, к.т.н., доц.
Григоренко Олена Григорівна _____

Рецензент:
Професор кафедри ІТМ, д.т.н., с.н.с.
Скуліш Марія Анатолієвна _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2021 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Леонід УРИВСЬКИЙ

«___»_____20__ р.

ЗАВДАННЯ
на дипломну роботу студенту
Вайлупову Владиславу Олексійовичу

1. Тема роботи «Застосування засобів протидії кіберзлочинності в телекомунікаційних мережах», керівник роботи Григоренко Олена Григорівна, кандидат технічних наук, доцент, затверджено наказом по університету від «14» квітня 2021 р. № 1007-с.

2. Термін подання студентом роботи 9 червня 2021 року.

3. Вихідні дані до роботи: Інформаційні матеріали щодо захисту та організації мереж. Структурований план порядку розробки матеріалів дипломної роботи.

4. Зміст роботи

Обґрунтувати актуальність теми. Розглянути питання міжмережевої взаємодії та процес аналізу кіберзагроз. Надати основні кіберзагрози, що можуть порушити цифрове благополуччя. Детально розглянути технічні засоби протидії кіберзлочинності. Показати причини необхідності впровадження освіти та навчання в галузі кібербезпеки. Роглянути переваги створення культури обізнаності про кібербезпеку. Проаналізувати питання необхідності політик та процедур безпеки. Розглянути спеціальні політики безпеки. У висновках відмітити особливості кожного розглянутого засобу протидії кіберзлочинності та визначити необхідність їх застосування.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):

Мультимедійна презентація для захисту дипломної роботи на тему: «Застосування засобів протидії кіберзлочинності в телекомунікаційних мережах»

6. Дата видачі завдання 15 квітня 2021 року.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
	Збір та вивчення документації. Перелік та огляд технологій та засобів, що використовуються для протидії кіберзлочинності в телекомунікаційних мережах.	15.04.2021	Виконано.
	Написання першого розділу дипломної роботи. Розгляд питання між мережевої взаємодії, процесу аналізу загроз кіберзлочинності, основних типів кіберзагроз.	08.05.2021	Виконано.
	Написання другого розділу дипломної роботи. Аналіз технічних засобів(програмно-апаратних, мережевих, хмартих) захисту від кіберзагроз.	16.05.2021	Виконано.
	Написання третього розділу дипломної роботи. Аналіз важливості питання впровадження освіти та навчання в області кібербезпеки. Огляд переваг створення культури обізнаності про кібербезпеку.	20.05.2021	Виконано.
	Написання четвертого розділу дипломної роботи. Розгляд політик та процедур безпеки. Огляд спеціальних політик безпеки.	30.05.2021	Виконано.
	Написання вступу та висновків до дипломної роботи.	04.06.2021	Виконано.
	Чистовий варіант дипломної роботи.	08.06.2021	Виконано.

Студент Владислав ВАЙЛУПОВ

Керівник Олена ГРИГОРЕНКО

АНОТАЦІЯ

Дипломну роботу виконано на 83 аркушах, вона містить перелік на використані джерела з 15 найменувань. У роботі наведено 14 рисунків.

Метою даної дипломної роботи є аналіз засобів що застосовуються для протидії кіберзлочинності в телекомунікаційних мережах.

У дипломній роботі розглянуто питання мережевої взаємодії, аналіз загроз кіберзлочинності та основні типи загроз. Розглянуті технічні засоби захисту безпеки, а саме програмно-апаратні засоби, мережні засоби та хмарні засоби. Проаналізовано, які переваги надає впровадження освіти та навчання в галузі кібербезпеки. Розглянуто питання необхідності політик та процедур безпеки.

МЕРЕЖА, ЗАГРОЗА, КІБЕРБЕЗПЕКА, ЗАХИСТ

ABSTRACT

This senior thesis is presented on 83 pages. It contains bibliography of 15 references. 14 figures are presented in senior thesis.

The purpose of this thesis is to analyze the methods used to combat cybercrime in telecommunications networks.

The thesis deals with the issues of network interaction, analysis of cybercrime threats and the main types of threats. Also in the thesis considered technical means of security protection, such as software and hardware means, network means and cloud means. The advantages of the introduction of education and training in the field of cybersecurity are analyzed. The need for security policies and procedures is considered.

NETWORK, THREAT, CYBER SECURITY, PROTECTION

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AES advanced encryption standard, стандарт розширеного шифрування.

API application programming interface, прикладний програмний інтерфейс.

DDoS (distributed) *denial-of-service*, розподілена атака на відмову в обслуговуванні.

DLCI data link connection identifier, ідентифікатор з'єднання каналу передачі даних.

DNS domain name system, система доменних імен.

DSL digital subscriber line, цифрова абонентська лінія.

EAP extensible authentication protocol, розширюваний протокол аутентифікації.

FTP file transfer protocol, протокол передавання файлів.

HIPS host-based intrusion prevention system, хост-орієнтована система запобігання вторгненням.

IaaS infrastructure-as-a-service, інфраструктура як послуга.

IDEA international data encryption algorithm, міжнародний стандарт шифрування даних.

IDS *intrusion detection* system, система виявлення атак (вторгнень).

IoT *internet of things, інтернет речей.*

IPS intrusion prevention system, система запобігання вторгнень.

ISDN integrated services digital network, цифрові мережі з інтегральними (вбудованими) послугами.

LAN local area network, локальна комп'ютерна мережа.

MIME multipurpose internet mail extensions, багатоцільові розширення для інтернет-пошти.

MITM *man in the middle, a*така посредника.

mVPN mobile VPN, мобільний VPN.

NAC network access control, контроль доступу в *мережу.*

PaaS platform as a service, платформа як послуга.

PGP pretty good privacy, шифруючи програмне забезпечення.

SaaS software as a service, програмне забезпечення як послуга.

SecaaS secuity as a service, безпека як послуга.

SIEM security information and event management, управління інформаційною безпекою та управління подіями безпеки.

SLA *service level agreement,* Угода про рівень послуг.

SPAN switched port analyzer, зеркалювання трафіку.

SQL structured query language, мова структурованих запитів.

SSH secure shell, безпечна оболонка.

SSID service set identifier, унікальне найменування бездротової мережі.

SSL secure sockets layer, рівень захищених сокетів.

TCO total cost of ownership, сукупна вартість володіння.

TCP transmission control protocol, протокол керування передачею.

TKIP temporal key integrity protocol, протокол цілісності тимчасового ключа.

UDP user datagram protocol, протокол датаграм користувача.

URL uniform resource locator, уніфікований локатор ресурсів.

VPN virtual private network, віртуальна приватна мережа.

WAF *web application firewall, фаєрвол веб-програм.*

WAN wide area network, глобальна мережа.

WEP wired equivalent privacy, стандарт захисту бездротового трафіку.

ЕЦП електронний цифровий підпис.

ІБ інформаційна безпека.

ІС інформаційна система.

ІТ інформаційні технології.

МЕ між мережевий екран.

ОС операційна система.

ПЗ програмне забезпечення.

ПК персональний комп’ютер.

ВСТУП

Швидке зростання глобальної мережі Internet і стрімкий розвиток інформаційних технологій привели до формування інформаційного середовища, що впливає на всі сфери людської діяльності. Нові технологічні можливості полегшують поширення інформації, підвищують ефективність виробничих процесів, сприяють розширенню ділових відносин. Однак, незважаючи на інтенсивний розвиток комп'ютерних засобів і інформаційних технологій, вразливість сучасних інформаційних систем і комп'ютерних мереж, нажаль, не зменшується. Тому проблеми забезпечення інформаційної безпеки привертають пильну увагу як фахівців в області комп'ютерних систем і мереж, так і численних користувачів, включаючи компанії, що працюють в сфері електронного бізнесу.

Зараз безпечна мережа стала потребою будь-якої організації. Загрози безпеці зростають із кожним днем, а високошвидкісні дротові та бездротові мережі та Інтернет-послуги стають небезпечними та ненадійними. Потреба також спрямована на такі сфери, як оборона, де безпечний доступ до ресурсів є ключовим питанням, що стосується інформаційної безпеки.

Актуальність теми дипломної роботи полягає в тому, що неможливо досягти необхідного рівня безпеки комп'ютерних систем і мереж без знання і компетентного застосування сьогоденних технологій, стандартів, протоколів і засобів забезпечення кібербезпеки.

Метою роботи є аналіз засобів, що застосовуються для протидії кіберзлочинності в телекомунікаційних мережах.

Об’єктом дослідження в роботі є питання кібербезпеки телекомунікаційних мереж.

Предметом дослідження в роботі є засоби протидії кіберзлочинності в телекомунікаційних мережах.

В роботі поставлені наступні завдання: розглянути питання мережевої взаємодії, аналізу кіберзагроз та основні загрози кібербезпеки. Проаналізувати технічні засоби захисту, а саме:

— Програмно-апаратні засоби(брандмауер, засоби виявлення та запобігання вторгненням, Honeypot, служби фільтрування контенту).

— Мережеві засоби (технологія VPN, контроль мережевого доступу та безпека бездротової точки доступу).

— Хмарні засоби (SaaS, PaaS, IaaS, Secaas).

Дослідити питання впровадження освіти та навчання в галузі кібербезпеки, створення культури обізнаності про кібербезпеку. Розгянути питання необхідності політик та процедур безпеки, проаналізувати спеціальні політики безпеки.

1 ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

1.1 Введення в мережевий обмін

Взаємоз’єднання телекомунікаційних мереж - встановлення фізичного та/або логічного з’єднання між різними телекомунікаційними мережами з метою забезпечення можливості споживачам безпосередньо або опосередковано обмінюватись інформацією. [1]

Комп’ютерна мережа - це електронне підключення комп’ютерів з метою обміну інформацією. Такі ресурси, як файли, програми та програмне забезпечення, є загальною інформацією, якою обмінюються в мережі. Перевагу мережевих зв'язків можна чітко бачити з точки зору безпеки, ефективності, керованості та економічної ефективності, оскільки вона дозволяє організувати співпрацю між користувачами в широкому діапазоні. В основному мережа складається з апаратних компонентів, таких як комп'ютер, концентратори, комутатори, маршрутизатори та інші пристрої, які відіграють важливу роль у передачі даних з одного місця в інше за допомогою різних технологій, таких як радіохвилі та дроти. У мережевих галузях доступно багато типів мереж, і найпоширенішою мережею є локальна мережа (LAN – Local Area Network) та глобальна мережа (WAN - Wide Area Network). Мережа LAN складається з двох або більше комп'ютерів, з'єднаних між собою на короткій відстані (до 2 км). WAN - це мережа, яка охоплює ширшу територію, більше 100 км, ніж локальна мережа. Кілька основних локальних мереж можна з'єднати разом, щоб сформувати глобальну мережу.

Інтернет - всесвітня інформаційна система загального доступу, яка логічно зв’язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами. [1]

Крім послуг з передачі інформації для різних абонентів, Інтернет-мережа надає також досить великий набір високорівневих частовикористовуваних сервісів:

— всесвітня павутина World Wide Web;
— доменні імена DNS;
— FTP-сервіси;
— email-сервіси;
— телеконференції;
— сервіси спілкування;
— пошук інформації в Інтернеті.

Побудова комп'ютерних мереж означає передусім використання моделі ISO/OSI, стека TCP/IP для передавання даних і технології Web для їх презентації.

Модель ISO/OSI вирішує питання зв’язку за допомогою багаторівневого підходу, що формує набір протоколів. Кожен рівень, що має справу з певним аспектом зв'язку, реалізується з протоколом, і ці протоколи співпрацюють між собою для вирішення завдання зв'язку. Модель взаємозв'язку відкритих систем (OSI) - це абстрактне подання основних рівнів, задіяних для вирішення проблеми зв'язку. [2]

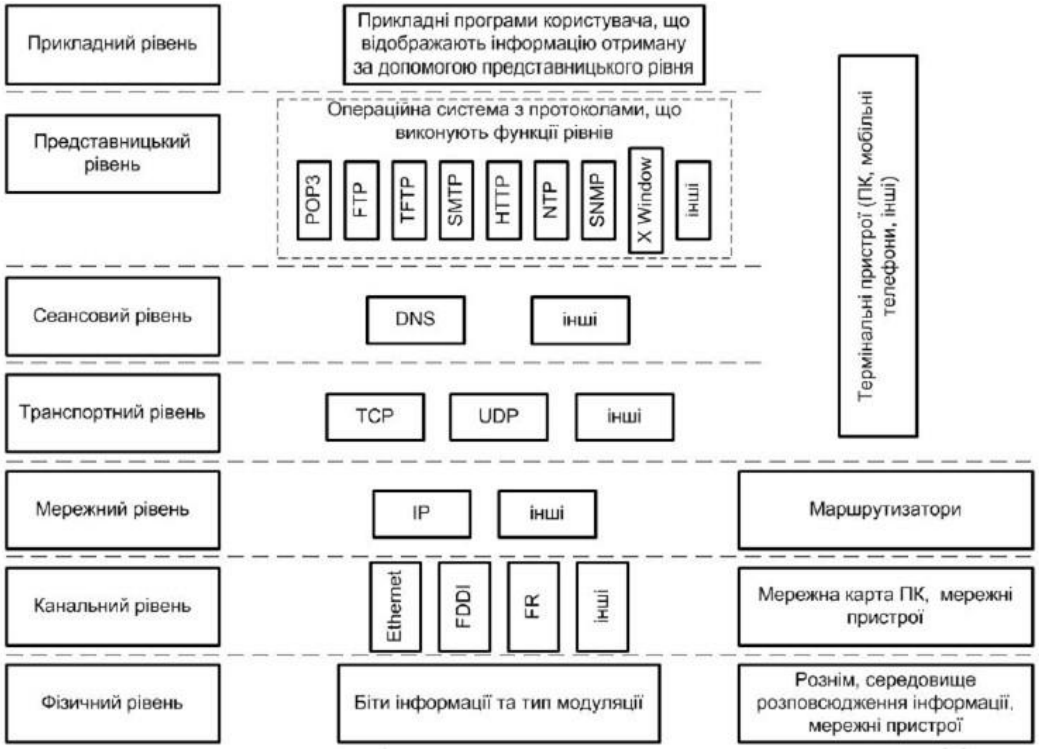

Рисунок 1.1 - Модель ISO/OSI та її реалізація

Прикладний рівень вказує, як певна програма використовує мережу і контактує з програмою, яка працює на віддаленій машині. Рівень представлення даних займається трансляцією або поданням даних на двох кінцевих хостах зв'язку. Сеансовий рівень відповідає за встановлення сеансу зв'язку з віддаленою системою, а також вирішує проблеми безпеки, такі як аутентифікація, перш ніж користувач програми зможе підключитися до віддаленої системи. Транспортний рівень забезпечує наскрізну, надійну або швидку роботу, доставку пакетів даних у відповідному порядку, а також підтримку контролю потоку. Мережевий рівень має справу з переадресацією пакетів даних від джерела до вузлів призначення комунікації. Канальний рівень займається пакуванням даних у кадри та забезпечує надійну доставку даних на фізичному носії. Фізичний рівень забезпечує кодування / декодування та модуляцію / демодуляцію для фактичної передачі даних через фізичний носій у вигляді послідовності бітів. [2]

Семирівнева модель OSI є концептуальною: вона показує різні дії, необхідні для зв'язку між прикладними програмами, що працюють на двох

різних хостах. Повна його реалізація призведе до надмірних накладних витрат і величезних затримок у доставці даних у пункті призначення. Модель TCP/IP є загальновживаною моделлю для комунікацій. Модель TCP/IP складається з чотирьох шарів: Прикладний, Транспортний, Мережевий та Управління доступом до мережі (Рівень мережевих інтерфейсів) (рис.1.2). Прикладний рівень моделі TCP/IP відповідає за обов'язки прикладного, рівня представлення даних та сеансового рівня моделі OSI. Транспортний рівень моделі TCP/IP подібний до транспортного рівня моделі OSI. Мережевий рівень піклується про адресацію та маршрутизацію пакетів даних через різні мережі. Кожен пристрій в мережі має унікальну IP-адресу. Рівень Управління доступом до мережі моделі TCP/IP поєднує в собі функціональність канального та фізичного рівня моделі OSI. Цей рівень підтримує організацію даних у кадри та їх кодування / декодування. Структура та передача кадрів залежить від топології та апаратної технології, що використовуються у мережі. IP-пакет даних позначається сегментом, дейтаграмою на транспортному рівні моделі OSI та фреймом на рівні Управління доступом до мережі відповідно. [3]

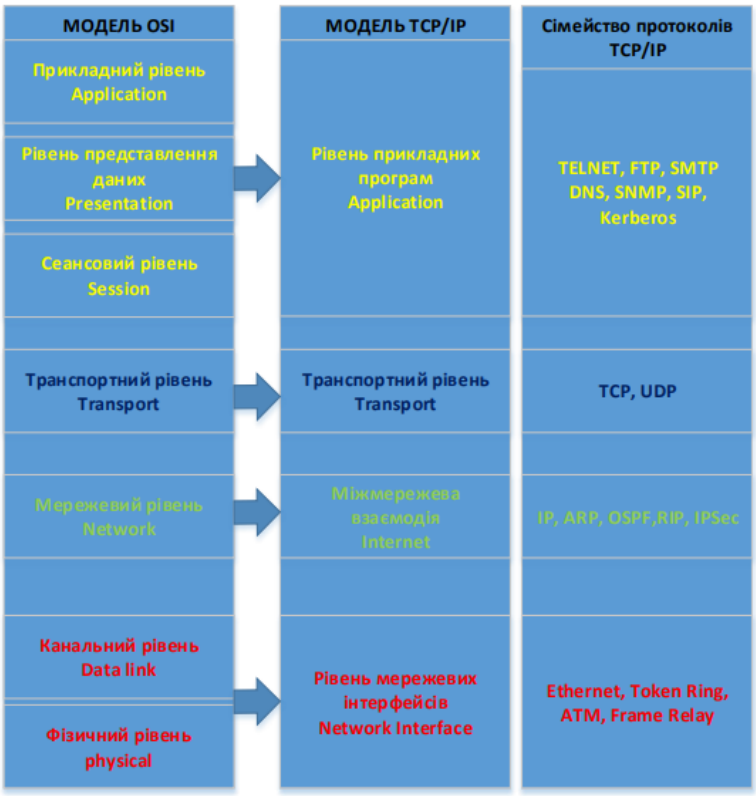

Рисунок 1.2 - Рівні моделі OSI, TCP/IP та сімейства протоколів TCP/IP

Двома часто використовуваними протоколами транспортного рівня в стеку протоколів TCP/IP є протокол управління передачею (TCP) та протокол дейтаграми користувача (UDP). TCP забезпечує надійну доставку даних у порядку. UDP забезпечує швидкі послуги для наскрізної доставки даних.

1.2 Аналіз загроз мережевої безпеки

Аналіз кіберзагроз - це процес оцінки кібердіяльності та можливостей невідомих кіберзлочинців. Згідно Закону України Про основні засади забезпечення кібербезпеки України термін кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів [4] . Це може бути порушенням шляху зв'язку, пошкодженням даних або крадіжкою даних.

Кіберзагрози зростають з кожним днем, оскільки технологічний прогрес у штучному інтелекті або інтелектуальних системах полегшує потребу в кращих навичках для обходу високозахищених систем. З цих причин необхідно проводити ретельний та детальний аналіз кіберзагроз, щоб знати ступінь їх загрози.

Основною метою аналізу кіберзагроз є отримання висновків, які допомагають ініціалізувати або підтримати розслідування. Потім вживаються заходи щодо усунення загрози з боку певних організацій, бізнесу чи державної системи. Аналіз загроз відповідає фактичним чи реальним кібератакам.

Остаточний результат оцінки загрози повинен забезпечувати найкращі практики щодо використання захисних засобів контролю для підвищення цілісності, доступності та конфіденційності, не впливаючи на функціональність та умови використання.

У кожній добре структурованій організації існують процедури та політики, які визначають, як здійснюється робота людей, машин та інших компонентів організації. Все це має бути чітко викладено з метою дотримання вимог.

На етапі збору даних першим кроком є збір інформації про фактичні випадки кібератаки або загрози. Прикладами можуть бути фішинговий заголовок, вміст електронної пошти, розкрита ворожа інфраструктура управління IP-адресами та іменами доменів, URL-адреси шкідливих посилань тощо. Сфера застосування повинна допомогти відфільтрувати сприйняті загрози, щоб забезпечити фокус на цілеспрямованих загрозах, які існують насправді.

Слід проаналізувати корпоративні процедури та політику та провести ретельне дослідження, щоб визначити, чи відповідають вони стандартам.

Далі перевіряється зібрана інформація, щоб визначити ступінь поточного впливу. На цьому етапі слід подвійно перевірити, чи є заходи

безпеки та політики адекватними захисними заходами. Тести на проникнення також проводяться в рамках аналізу вразливості з метою ідентифікації загроз.

Аналіз загрози - це безперервний процес, а не випадковий або разовий випадок. Це постійний процес, який забезпечує належну роботу всіх захисних механізмів. Оцінка ризику повинна бути включена як невід'ємна частина роботи організації, щоб вона стала частиною загального життєвого циклу. Це допомагає визначити ризики, які, можливо, ще не досягли повноцінної стадії, коли вони завдають організації максимальної шкоди та збитків. [5]

Після завершення попередніх кроків використовується визначений блок загроз для визначення превентивних заходів. Завдання на цьому етапі - класифікувати дані загрози за групами, розподілити кожен шаблон до конкретних суб'єктів загрози та вжити заходів щодо пом'якшення наслідків. Послідовно передбачається можливість появи подібних атак у майбутньому.

Аналіз кіберзагроз - це постійний процес, який слід проводити часто, щоб забезпечити ефективну роботу заходів безпеки відповідно до намірів. Це пов'язано з швидко мінливими технологіями та іншими факторами, що впливають на кіберпростір, такими як політичні фактори, соціальні фактори тощо. Організації, які не проводять аналіз загроз та ризиків, залишаються відкритими для нападу кіберзлочинців, які можуть призвести до збитку їх бізнесу.

1.3 Типові загрози кібербезпеки та їх розповсюдження

Загрози інформаційної безпеки можна розділити на два типи: технічні загрози і загрози, що виникли із-за людського фактору.

1.3.1 Зловмисне програмне забезпечення

Зловмисне програмне забезпечення зазвичай встановлюється в систему, коли користувач натискає шкідливе посилання або електронну пошту. Шкідливе програмне забезпечення може бути доставлено різними способами. Після встановлення шкідливе програмне забезпечення може блокувати доступ до важливих компонентів вашої мережі, пошкодити вашу систему та збирати конфіденційну інформацію.

Шпигунське програмне забезпечення - це програмне забезпечення, яке дозволяє користувачеві отримувати інформацію про діяльність вашого комп’ютера шляхом таємної передачі даних з вашого жорсткого диска.

Програма-вимагач – це вид шкідливого програмного забезпечення, призначений для шифрування файлів на пристрої, роблячи будь-які файли непридатними для використання. Зазвичай зловмисники вимагають грошового викупу в обмін на розшифровку.

Back door надає віддалений доступ до ресурсів у програмах, таких як бази даних та файлові сервери. При цьому зловмисники мають можливість віддалено видавати системні команди та оновлювати шкідливе програмне забезпечення.

Троянські програми – це тип шкідливого програмного забезпечення або коду, який діє як законна програма чи файл, щоб змусити користувача завантажити та виконати шкідливе програмне забезпечення на його пристрої. Мета полягає в тому, щоб пошкодити або вкрасти дані вашої організації або нанести будь-яку іншу шкідливу дію у мережі.

Черв’яки – це тип шкідливого програмного забезпечення, яке поширює свої копії з комп’ютера на комп’ютер без будь-якої взаємодії з людьми, і їм не потрібно прив’язуватися до програмного забезпечення, щоб заподіяти шкоду.

1.3.2 Фішинг

Фішинг – це вид соціальної інженерії, який намагається обдурити користувачів в обхід звичайних практик кібербезпеки. Мета – здобуття конфіденційних даних, таких як імена користувачів та паролі, інформація про банківські рахунки, номери соціального страхування та дані кредитних карток.

Як правило, хакери відправляють електронні листи, які, здається, приходять від надійних відправників. Кіберзлочинці намагаються змусити користувачів натискати на посилання в повідомленнях, які будуть перенаправляти їх на шахрайські веб-сайти, які запитують особисту інформацію або встановлюють шкідливе ПЗ.

1.3.3 Розподілена відмова в обслуговуванні (DDoS)

Denial Of Service (відмова в обслуговуванні) - особливий тип атак, спрямований на виведення мережі або сервера з робочого стану.

Під час цієї атаки запити надходять із сотень або тисяч IP-адрес. Ці атаки часто навантажують канал трафіком і сповільнюють проходження даних, а іноді і повністю блокують передачу по ньому корисної інформації.

1.3.4 Атаки типу "людина посередині" (MITM)

Ці атаки трапляються, коли зловмисники стають посеред двостороннього спілкування. Вони фільтрують та викрадають конфіденційну інформацію та можуть повертати сфабриковані відповіді користувачеві.

Кінцевою метою атак MITM є отримання доступу до даних вашого бізнесу або клієнтів.

1.3.5 Введення структурованої мови запитів (SQL)

Підроблена база даних служить для спостереження за уразливими ПЗ і для виявлення атак, що використовують ненадійну архітектуру систем або метод SQL-ін'єкції, які експлуатують SQL-служби або засновані на зловживанні привілеями. [5]

1.3.6 Уразливості, викликані людським фактором

Група незадоволених співробітників може бути дуже небезпечною, тому що багато хто з співробітників компанії має доступ до важливої інформації. Особливу групу складають співробітники, такі як системні адміністратори, що можуть залишити "чорні ходи" для подальшої можливості використання ресурсів, викрадення конфіденційної інформації.

Велика кількість зловживань може бути викликана халатними діями співробітників. Наприклад, не встановлення необхідних оновлень, не змінення налаштувань «за замовчуванням» і несанкціоновані методи виходу через мережу компанії в Internet. В результаті цих дій злочинці здобувають доступ в захищену приватну мережу.

Низька кваліфікація також може призвести до катастрофічних наслідків. Із-за недостатньої кваліфікації користувач не може зрозуміти, з чим він має справу. Тому навіть найліпші засоби захисту не можуть забезпечити необхідну безпеку. Більшість таких людей не усвідомлюють реальної загрози від запуску зловмисних файлів і програм та не розрізняють, яку інформацію слід захищати. [5]

1.4 Висновки до розділу 1

У першому розділі розглянуті питання мережевої взаємодії, важливість аналізу кіберзагроз та типові загрози кібербезпеці.

Основу мережевої взаємодії складають моделі ISO/OSI та TCP/IP. Вони розділяють питання обміну інформації на рівні, кожен з яких має справу з певним аспектом зв’язку та реалізується певними протоколами.

Аналіз загроз кібербезпеки є одним із головних процесів забезпечення безпеки, адже саме завдяки аналізу можна ввести превентивні заходи та забезпечити захист від можливих загроз, що можуть призвести до збитків. До аналізу загроз входять: збір фактичної інформації про кібератаки та загрози, перевірка інформації та оцінка поточного впливу, аналіз процедур та політик безпеки на відповідність стандартам безпеки, введення превентивних заходів.

Також, під час розглядання загроз кібербезпеки, визначено, що основну небезпеку складають не тільки технічні загрози(шкідливе програмне забезпечення, фішинг, DDoS атаки, SQL-ін’єкції, атаки типу «людина посередині»), а й загрози, викликані людським фактором(незадоволені, халатні чи низькокваліфіковані співробітники).

2 ТЕХНОЛОГІЇ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

2.1 Апаратні та програмні засоби захисту

Засоби захисту інформації - це лінійка пристроїв і пристосувань, приладів та технічних систем, а також інших виробів, що застосовуються для вирішення різних завдань із захисту інформації.

Технічні (апаратні) засоби захисту інформації - це різні пристрої, що на рівні обладнання вирішують завдання інформаційного захисту.

Існує кілька апаратних технологій, що використовуються для захисту даних організацій:

— Брандмауер
— Спеціалізовані системи виявлення вторгнень
— Системи запобігання вторгненням
— Служби фільтрування контенту
— Honeypot

2.1.1 Брандмауер

Брандмауер – це міжмережевий екран, який послідовно фільтрує дані, що проходять через нього. За допомогою певних правил або шаблонів він аналізує трафік, який надходить з боку мережі або від вашого комп'ютера. Якщо пакет не пройшов перевірку, він не зможе перетнути брандмауер і потрапити з інтернету на пристрій користувача.

Міжмережеві екрани встановлюють не тільки на комп'ютерах користувачів, а й на серверах або на маршрутизаторах між підмережами. Це потрібно, щоб підозрілий трафік не міг швидко розповсюдитися по всій мережі.

Брандмауери бувають програмними (Software) і програмно-апаратними (програмне забезпечення (ПЗ) і пристрій, на якому воно працює). Перші є більш доступними, але займають частину ресурсів комп'ютера і не такі

надійні. Для рядових користувачів їх цілком достатньо. Другі – це зазвичай корпоративні рішення, які встановлюють у великих мережах з підвищеними вимогами до безпеки. [6]

Брандмауер може захистити від таких атак:

— Фішинг.

— Доступ через Back door. Злам з використанням віддаленого робочого столу. Атаки такого формату дозволяють отримати доступ до комп'ютера по мережі і керувати ним. Брандмауер помітить підозрілий трафік і заборонить його передачу.

— Переадресація пакетів

— DDoS-атаки.

Для захисту від несанкціонованого мережевого доступу міжмережевий екран розташовується між зовнішньою мережею та між мережею організації. При цьому увесь трафік має проходити тільки через міжмережевий екран (рис.2.1).

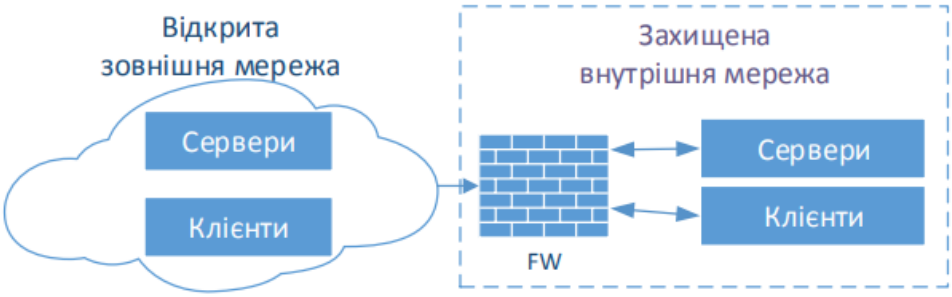

Рисунок 2.1 - Схема підключення міжмережевого екрану

Міжмережевий екран (МЕ), до якого підключено безліч вузлів внутрішньої мережі, вирішує такі задачі:

— Задачу обмеження доступу зовнішніх засобів до внутрішніх ресурсів;

— Задачу розмежування доступу користувачів внутрішньої мережі до зовнішніх ресурсів. [7]

2.1.2 Спеціалізовані системи виявлення та запобігання вторгненням

У сучасному світі системи виявлення та запобігання вторгненням (Intrusion detection system / Intrusion prevention system , IDS / IPS) - необхідний елемент захисту від мережевих атак. Основне завдання даних систем - виявлення фактів несанкціонованого доступу в корпоративну мережу або несанкціонованого управління нею, з виконанням відповідних заходів протидії (інформування адміністраторів про факт вторгнення, обрив з'єднання або перенастроювання брандмауера для блокування подальших дій зловмисника і т.д.).

Система IPS (Intrusion Prevention System) призначена для запобігання атак (рис.2.2). Вона є підкласом IDS-систем. Така система стежить за трафіком і блокує підозрілі потоки даних. Її мета – виявити і запобігти несанкціонованим діям в мережі. Система використовує набір правил, щоб заблокувати трафік. Таким чином, вона блокує прогалини в безпеці. IPS застосовується на межі мережі або в окремих хостах. Вона може використовувати дублювання трафіку (SPAN) і не мати IP-адреси, залишаючись невидимою для зловмисника. [8]

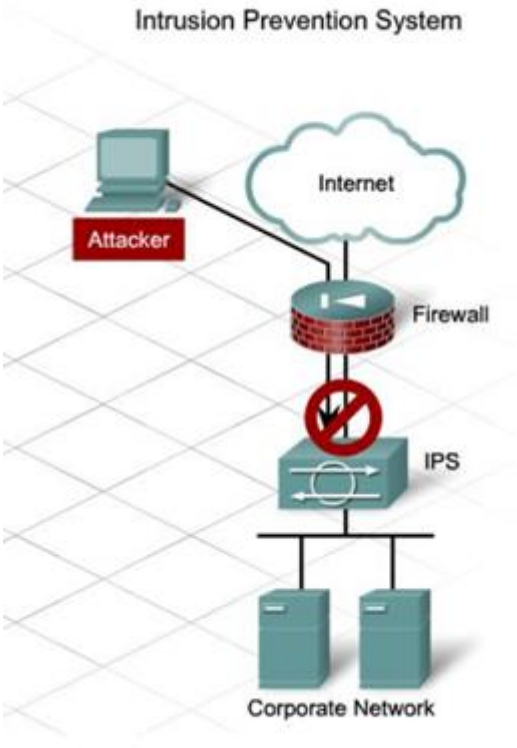

Рисунок 2.2 - Система запобігання вторгненням

IPS можна розділити на два класи. Перший клас (IPS) аналізує трафік і порівнює з відомими характеристиками загроз. Другий (HIPS) – аналізує протоколи і шукає заборонений трафік в базі знайдених раніше вразливостей. Саме цей клас забезпечує захист від невідомих атак.

Система IDS (Intrusion Detection System) використовується для виявлення нетипових дій в мережі та попередження про них фахівця з інформаційної безпеки (ІБ) (рис.2.3). Повідомлення виводиться на панель управління або відправляється на пошту, телефон тощо. Мета системи – моніторинг трафіку і знаходження мережевих атак, а також виявлення порушень користувачами політики безпеки. Системи виявлення вторгнень IDS допомагають відслідковувати стан справ з боку безпеки.

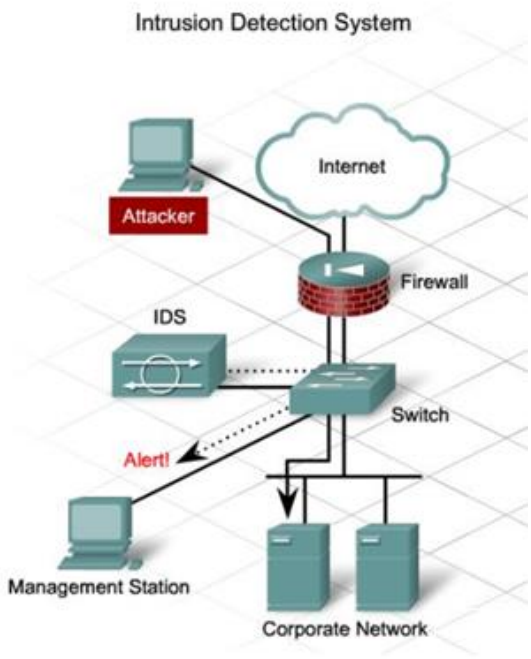

Рисунок 2.3 - Система виявлення вторгнень

Функції IDS-систем:

— запис інформації – відправка в системи збору логів або SIEM-системи;

— повідомлення про інциденти (alert-повідомлення);

— складання звітів – підсумовуються всі дані щодо подій.

Зазвичай архітектура IDS включає в себе:

— підсистему сенсорів, призначену для збору подій на різних ділянках захисту системи;

— підсистему аналізу, призначену для виявлення і класифікації атак і підозрілих дій на основі даних сенсорів;

— сховище, що забезпечує накопичення первинних подій і результатів аналізу ;

— консоль управління, що дозволяє конфігурувати IDS, спостерігати за станом системи, переглядати звіти про інциденти, що виявлені системою.

Існує два основні підходи до виявлення вторгнень:

— сигнатурний;

— поведінковий.

Сигнатурний аналіз трафіку в IDS дуже схожий на принцип роботи багатьох антивірусів. Мережевий трафік аналізується і порівнюється з базою даних сигнатур, в якій зберігається інформація про шкідливі програми, якщо в трафіку виявляється шкідливий об'єкт, система сповіщає про це відповідальну особу.

Поведінковий аналіз полягає в тому, що включена в мережу IDS досліджує нормальну поведінку і функціонування користувачів і додатків в мережі, і потім, на підставі побудованої моделі система виявляє некоректну і аномальну поведінку. [8]

2.1.3 Служби фільтрування контенту

Фільтрація контенту – популярна технологія, яку використовують антивіруси і фільтри спаму, засоби захисту від нецільового використання мережевих ресурсів і системи захисту від витоків.

Технології контентної фільтрації сьогодні використовуються в самих різних рішеннях IT-безпеки. Використання інтернет-фільтрації значно збільшує безпеку локальної мережі, так як дозволяє забезпечити адміністративний контроль за використанням інтернету, завантаженнями і забезпечує блокування відвідування потенційно небезпечних ресурсів, а також, коли це необхідно, сайтів, не пов'язаних з роботою (рис.2.4).

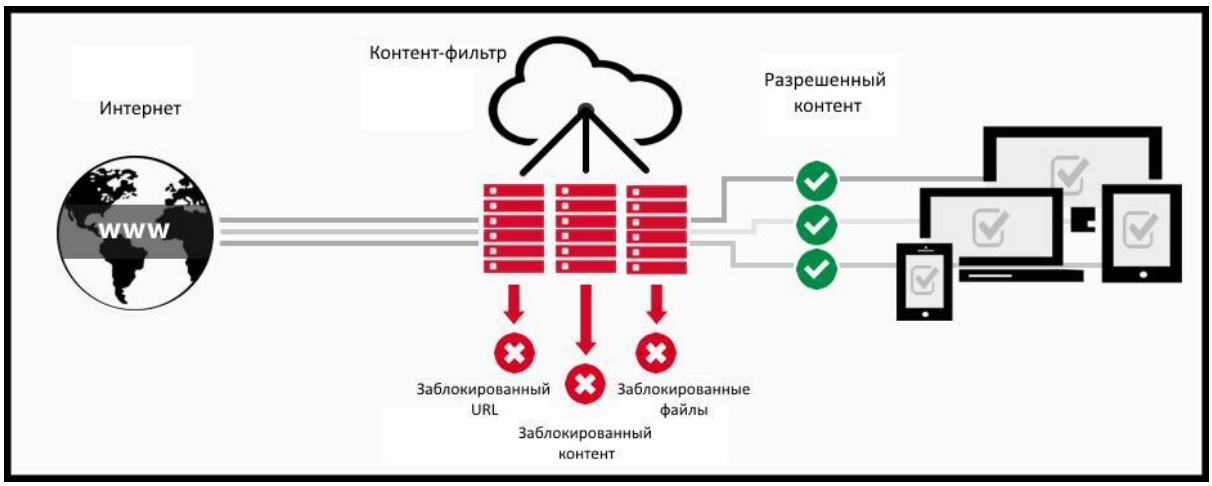

Рисунок 2.4 - Схема організації контент-фільтру на прикладі мережі

Фільтрацію контенту можна розділити на два основних напрямки: фільтрація веб-контенту і фільтрація електронної пошти. Такий поділ обумовлено тим, що зазначені канали передачі інформації є основними каналами доставки контенту кінцевим користувачам.

Слід зазначити, що контент-фільтр відрізняється від антивірусного фільтра, так як він працює безпосередньо з контентом (інформацією, призначеної для людини), що міститься в електронному листі або на веб-сторінці, а не з кодами файлів (як у випадку з антивірусним фільтром). Завданням контент-фільтра є блокування електронного повідомлення або веб-сторінки, які відповідають або не відповідають певним умовам. Таких умов може бути безліч, вони представлені далі:

— Блокування веб-сторінок по чорному / білому списку. У разі коли фільтра за категоріями недостатньо або, якщо сайт помилково віднесений до невірної категорії, адміністратор може скласти чорний і білий списки сайтів, які завжди повинні бути заборонені або завжди дозволені.

— Антиспам – найбільш поширений модуль контент-фільтра. Ось уже багато років, намагаючись боротися зі спамом, виробники рішень інформаційної безпеки винаходять все більш складні і досконалі технології. Роботу антиспамового модуля можна описати таким чином: спеціальний алгоритм оцінює електронне повідомлення відразу за кількома параметрами,

на підставі чого робить висновок, є лист «корисним» для користувача або спамом.

— Блокування електронних повідомлень або веб-сторінок за словами або словосполученнями, що містяться в їх заголовках, в тілі листа або на самій сторінці. Використовуючи цей механізм, адміністратор може вказати «заборонені» слова або фрази. Якщо приходить лист, що містить таке слово, то по відношенню до нього система зробить відповідні дії (заблокує доставку, видалить лист і т.д.). Аналогічно система відреагує і в тому випадку, якщо користувач намагається відкрити веб-сайт, що містить таке слово, цей сайт буде негайно заблокований.

— Блокування файлів, вкладених в лист або скачуваних з веб-сторінки, за назвою або розширенням. Адміністратор може вказати частину імені файлу або його розширення, за якими буде здійснюватися блокування. Наприклад, більшість контент-фільтрів блокують виконувані розширення .com і .exe в поштових вкладеннях, так як це популярний метод зараження ПК вірусами.

— Блокування листів, веб-сайтів або файлів, які не відповідають певним форматам. Багато рішень надають список певних форматів, які часто не дотримуються зловмисниками при розсилці шкідливого контенту, або є ймовірною його ознакою. Наприклад, подвійні розширення файлів, некоректний тип MIME(Multipurpose Internet Mail Extension), зашифровані архіви тощо. [5]

2.1.4 Honeypot

У комп'ютерному світі терміном honeypot називають пастки для хакерів. Це системи, які заманюють кіберзлочинців в пастку. Зловмисники атакують приманку, і фахівці користуються цим, щоб зібрати інформацію про методи угруповання або відволікти зловмисників.

Пастка імітує комп'ютерну систему з програмами та даними, і кіберзлочинці приймають її за справжню ціль. Наприклад, honeypot може імітувати систему для виставлення рахунків клієнтам компанії. Це популярна мішень серед кіберзлочинців, що хочуть дістати номера кредитних карт. За хакерами, що потрапили в пастку можна спостерігати, щоб, вивчивши їх поведінку, створити більш ефективні способи захисту справжніх систем.

Щоб зробити пастки більш привабливими для зловмисників, їх навмисно роблять уразливими. Наприклад, використовують порти, які можна виявити за допомогою сканування, або ненадійні паролі. Уразливі порти часто залишають відкритими: так ростуть шанси, що приманка спрацює і злочинець відвернеться від захищених реальних мереж.

Пастка – не антивірус і не мережевий екран, вона не допомагає вирішувати конкретні проблеми безпеки. Це скоріше інформаційний інструмент, який допомагає вивчити існуючі і виявити нові загрози. Використовуючи зібрані дані, можна пріоритезувати проблеми і правильно розподілити ІБ-ресурси.

Різні види кіберпасток використовуються для виявлення різних загроз. Їх властивості залежать від загрози, для якої вони створені. У кожної пастки своя роль в комплексній і ефективній стратегії кібербезпеки.

Поштові пастки, або пастки для спаму, поміщають підроблену електронну адресу в добре заховане розташування, де його може знайти тільки автоматичний збирач електронних адрес. З огляду на призначення такої адреси, можна бути на 100% впевненим, що будь-який лист, що прийде на цю пошту – спам. Всі листи, що потрапили в пастку, можна відразу блокувати, а IP-адресу відправника заносити у чорний список.

Підроблена база даних служить для спостереження за уразливими ПЗ і для виявлення атак, що використовують ненадійну архітектуру систем або метод SQL-ін'єкції, які експлуатують SQL-служби або засновані на зловживанні привілеями.

Пастка для шкідливого ПЗ імітує додатки і API, заохочуючи атаки шкідливих програм. Атакуючі програми піддаються аналізу для розробки захисту або усунення уразливостей в API.

Пастка для «павуків» ловить пошукових роботів (так званих «павуків»), створюючи веб-сторінки і посилання, доступні тільки їм. З її допомогою вчаться блокувати шкідливих ботів і рекламних пошукових роботів.

Аналізуючи вхідний трафік пастки, можна:

— з'ясувати місцезнаходження кіберзлочинців;

— оцінити ступінь загрози;

— вивчити методи зловмисників;

— дізнатися, які дані або програми їх цікавлять;

— оцінити ефективність використовуваних заходів захисту від кібератак.

Кіберпастки також діляться на високоінтерактивні і низькоінтерактивні. Низькоінтерактивні пастки використовують менше ресурсів і збирають базову інформацію про рівень, тип загрози і її джерело. Для їх установки зазвичай потрібні лише деякі модельовані TCP- і IP-протоколи і мережеві служби. Але така пастка не затримає злочинця надовго і не дозволить детально вивчити його звички або складні загрози.

У той же час високоінтерактівні пастки змушують зловмисників витратити багато часу, а значить, дозволяють зібрати безліч даних про їхні цілі і наміри, методи роботи і про використовувані ними вразливості. Це дуже «липкі» пастки – злочинці надовго застряють в базах даних, системах і процесах. У цей час дослідники можуть відстежити, де саме в системі зловмисник шукає конфіденційну інформацію, за допомогою яких інструментів підвищує рівень доступу, які експлойти використовує для компрометації системи.

У кожного з цих двох типів пасток своє призначення: низькоінтерактивна надає базові відомості про загрози, а високоінтерактивна

доповнює їх інформацією про наміри і методи злочинців, а також про уразливості, які вони використовують.

Система аналізу загроз з використанням кіберпасток допомагає компаніям правильно розподіляти ІБ-ресурси і виявляти уразливості своїх інформаційних систем.

Переваги кіберпасток полягають у наступному: це відмінний спосіб знайти уразливості важливих систем. Наприклад, пастка може не тільки продемонструвати, наскільки небезпечні атаки на пристрої інтернету речей, але і підказати, як можна підсилити захист.

Є кілька причин використовувати пастки замість того, щоб намагатися виявити атаки на справжню систему. Так, в пастці за визначенням не може бути легітимної активності – будь-які зафіксовані дії, швидше за все, є спробою прозондувати систему або зламати її.

Можна легко виявити закономірності (наприклад, схожі або походять з однієї країни, IP-адреси), що свідчать про прочісування мережі. Такі ознаки атаки легко втратити на фоні звичайного інтенсивного трафіку у опорній мережі.

Крім того, кіберпастки споживають дуже мало ресурсів і трафіку. Їм не потрібно потужне обладнання.

Також кіберпастки дають мінімум хибно позитивних спрацьовувань. Знову ж таки, це допомагає фокусувати зусилля на важливих проблемах і не витрачати ресурси даремно. До речі, зіставляючи зібрані пасткою дані з даними журналів системи і мережевого екрану, можна налаштовувати IDS на пошук найбільш релевантних загроз, щоб знизити число хибно позитивних спрацьовувань. Таким чином, пастки допомагають удосконалювати інші системи кібербезпеки.

Кіберпастки формують докладне уявлення про розвиток загроз, вектори атак, експлойтів і шкідливі програми, а пастки для спаму – також про спамерів і фішингові кампанії. У той час, як злочинці постійно відточують свої методи, пастки допомагають виявляти все нові загрози і

вторгнення. Грамотно використовуючи пастки, можна усунути сліпі зони системи кібербезпеки.

Також пастки – прекрасний тренажер для співробітників ІБ-відділу, які можуть в контрольованому середовищі безпечно вивчати методи кіберзлочинців і різні типи загроз. При цьому вони можуть повністю зосередитися на атаках, не відволікаючись на справжній трафік.

2.2 Мережеві засоби захисту

2.2.1 Віртуальна приватна мережа (VPN)

Virtual Private Network (VPN) - узагальнена назва технологій, що дають можливість забезпечити одне чи більше мережевих з'єднань поверх іншої мережі. Термін віртуальної приватної мережі (VPN) став широко поширеним з виходом операційної системи Microsoft Windows 95. Основна ідея полягала в тому, щоб забезпечити співробітникам безпечний доступ до внутрішньої мережі організації, не відкриваючи мережі для атак хакерів.

Віртуальна приватна мережа заснована на трьох базових принципах: тунелювання, шифрування і аутентифікація. Тунелювання забезпечує передачу пакетів між мережевими вузлами відправника і одержувача так, що з точки зору працюючого на ньому ПЗ вони виглядають підключеними до однієї (локальної) мережі. Однак при цьому пакет даних проходить через безліч вузлів відкритої публічної мережі, тому для захисту даних використовується електронний цифровий підпис (ЕЦП) – це додатковий блок інформації, що передається разом з пакетом інформації та який виробляється відповідно до асиметричного криптографічного алгоритму і унікальний для вмісту пакета і секретного ключа ЕЦП відправника. Цей блок є ЕЦП пакету і дозволяє виконати аутентифікацію даних отримувачем, який знає відкритий ключ ЕЦП відправника, що і забезпечує захищеність даних. [9]

З урахуванням усього сказаного раніше, сформулюємо загальні вимоги до корпоративної VPN:

— Всі завдання адміністрування, як в частині завдання розмежувальної політики доступу до корпоративних ресурсів, так і в частині реалізації ключової політики (створення і поширення ключів шифрування віртуальних каналів), повинні вирішуватися безпосередньо адміністратором безпеки централізовано (до складу VPN повинно входити автоматизоване робоче місце адміністратора безпеки);

— Користувач повинен бути виключений зі схеми адміністрування – повинен працювати в корпоративній мережі "під примусом" адміністратора – повинен спілкуватися тільки з тими користувачами (або комп'ютерами), з якими йому дозволено адміністратором, при цьому повинен обмінюватися з ними даними тільки в тому вигляді (відкритими, або зашифрованими), в якому йому дозволено адміністратором. Як наслідок, шифрування віртуальних каналів має здійснюватися "прозоро" для користувача, ключ шифрування користувача (надається йому адміністратором) не повинен дозволяти порушити користувачеві конфіденційність даних при їх розкраданні.

Основними технологіями шифрування VPN є:

— IPsec

— SSL VPN

IPsec – комплект протоколів для забезпечення захисту даних, що транспортуються по протоколу IP. Дозволяє здійснювати підтвердження справжності (аутентифікацію), перевірку цілісності чи шифрування IP-пакетів. У IPsec також входять протоколи для захищеного обміну ключами в мережі інтернет. Як і стандартний VPN, IPSec є досить гнучким і добре налаштованим засобом, який можна використовувати для під'єднання двох мереж (або одного комп'ютера) до корпоративної мережі. Трафік, що передається по VPN такого типу, шифрується і захищається паролем для захисту від внесення змін на шляху від відправника до адресата (рис.2.5). Однак, хоча IPsec описують як стандартизовану технологію, деякі її реалізації можуть бути не особливо сумісними. Тому IPSec – хороший вибір

для компаній, у яких є ресурси на IT-персонал, здатний підтримувати такі протоколи.

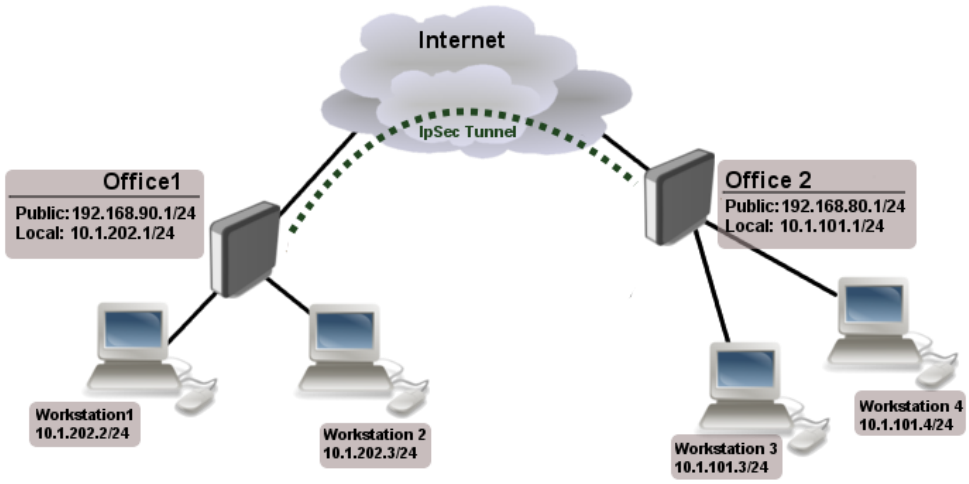

Рисунок 2.5 - Приклад організації VPN за допомогою IPsec

SSL (Secure Sockets Layer) - криптографічний протокол, який дозволяє забезпечити більш безпечний зв'язок. Він використовує симетричне шифрування для збереження конфіденційності, асиметричну криптографію для аутентифікації ключів обміну, коди аутентифікації повідомлень для цілісності повідомлень. Спочатку віртуальні приватні мережі на основі SSL розроблялися, як додаткові і альтернативні технології віддаленого доступу на основі IPsec VPN. Однак, такі фактори, як достатня надійність і дешевизна, зробили цю технологію привабливою для організації VPN. SSL VPN з'єднує одиночний комп'ютер з шлюзом в корпоративній мережі. Оскільки, в разі SSL VPN в якості інтерфейсу використовується браузер користувача, найчастіше йому не потрібно встановлювати додаткове ПЗ. Це, в свою чергу, спрощує установку і підтримку, а також дозволяє встановлювати з'єднання з комп'ютерами, що працюють під різними операційними системами. Мінусом тут є той факт, що, незважаючи на можливість роботи через браузер, VPN з'єднання через SSL можна використовувати тільки з додатками, що працюють з HTML / HTTP. Це обмеження можна обійти, встановивши на

клієнтський комп'ютер спеціальні додатки, але це буде обмежувати гнучкість, так що вигідніше, можливо, буде використання IPSec VPN.

Досить часто буває так, що працівники компанії повинні передавати конфіденційну інформацію, перебуваючи за межами офісу – для цього був розроблений mVPN. Головна його відмінність від звичайного VPN в тому, що кінцева точка, з якої встановлюється з'єднання, не є нерухомою, тому mVPN повинен вміти відновлювати захищене з'єднання при переході клієнта з однієї мережі в іншу. Для цього використовується протокол IPsec, за допомогою якого відбувається шифрування даних всередині VPN-каналу. Це дозволяє захистити з'єднання між віддаленим комп'ютером і основним шлюзом в головному офісі компанії.

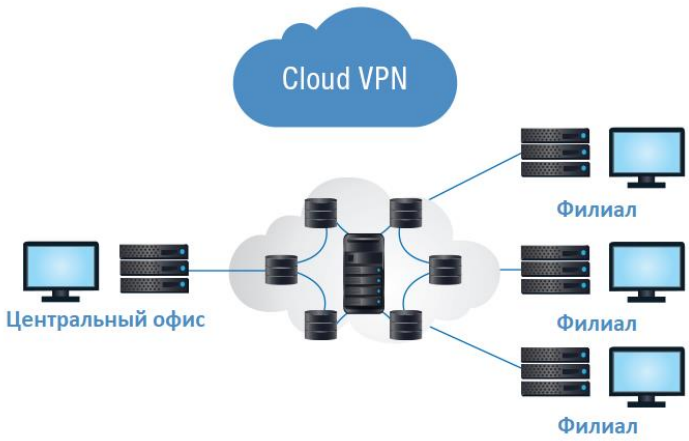

Рисунок 2.6 - Приклад організації VPN в хмарі

З розвитком хмарних технологій з'явилася можливість створити VPN в хмарі (рис.2.6) – це дозволяє відмовитися від сервера в організації, все налаштування може проходити віддалено. До того ж зазвичай плата за хмарні сервери йде погодинна, і в будь-який момент часу можна припинити використання сервера і платити тільки за місце на диску (зручно для компаній, які працюють, наприклад, 8-10 годин в день). Так само хмарний сервер легко масштабувати – знижувати або збільшувати кількість ресурсів сервера при зменшенні або зростанні числа користувачів. [10]

VPN дає можливість мільйонам людей і компаній в усьому світі безпечно передавати інформацію. Тому очевидно, що ця технологія в доступному для огляду майбутньому продовжить відігравати таку ж важливу роль.

2.2.2 Контроль мережевого доступу (NAC)

Контроль мережевого доступу (NAC) – це комплекс технічних заходів і засобів, який реалізує політики і правила доступу в мережу та забезпечує захист всіх кінцевих пристроїв, що мають до неї доступ від присутніх всередині загроз безпеки.

Для виконання вимог політик інформаційної безпеки на підприємствах відповідальні співробітники повинні контролювати облікові дані підключених до сервісів користувачів, інформацію про пристрій, з якого було вироблено підключення, і якими саме програмами співробітник може скористатися в рамках встановленої сесії. Системи NAC дозволяють виконувати це завдання і забезпечити централізоване управління і адміністрування політик доступу співробітників в інформаційному середовищі організації.

Дії NAC-системи полягають в тому, щоб з'ясувати, чи безпечно пристрій здійснює спроби підключення до мережі, і чи відповідає його конфігурація певним правилам доступу. Після процедури ідентифікації система приймає рішення про те, який рівень доступу до системних ресурсів необхідно надати.

Хоча в більшості компаній для аутентифікації користувачів застосовується управління аутентифікацією, авторизацією і розрахунків (AAA) і авторизації мережевих привілеїв, фактично відсутній спосіб аутентифікації профілю безпеки кінцевого пристрою, на якому працює користувач. Без точного способу оцінки "стану здоров'я" пристрою навіть найнадійніший користувач може ненавмисно піддати інших користувачів

мережі значному ризику, який виникає через присутність інфікованого або недостатньо захищеного від інфекцій пристрою.

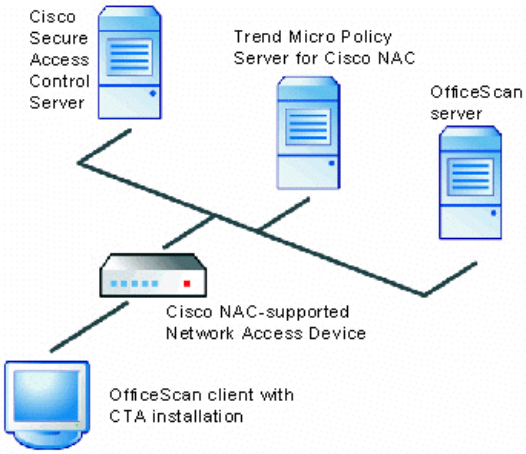

Рисунок 2.7 - Приклад підключення системи NAC до мережі

NAC використовує інфраструктуру мережі для контролю над дотриманням політики безпеки на всіх пристроях, які прагнуть отримати доступ до ресурсів мережі (рис 2.7). Цим шляхом знижується збиток, який можуть заподіяти виникаючі загрози безпеки. Використовуючи NAC, клієнти отримують можливість надавати мережевий доступ тільки тим, хто дотримується запропонованих вимог, безпечним кінцевим пристроям (наприклад, комп'ютерам і серверам) і обмежувати доступ для пристроїв, що не відповідають вимогам.

Впровадження NAC забезпечує, зокрема, такі переваги:

— Істотно зростає рівень безпеки в будь-якій мережі, незалежно від її розміру або складності структури. NAC допомагає простежити за дотриманням політики безпеки на всіх призначених для користувача мережевих пристроях. За рахунок превентивного захисту від черв'яків, вірусів, шпигунських і інших злочинних програм, компанії отримують можливість зосередити зусилля на профілактиці, а не на заходах у відповідь.

— Зростає стабільність роботи компаній і масштабованість, оскільки є можливість інспектування та контролю всіх пристроїв, що

з'єднуються з мережею, незалежно від того, який метод доступу вони використовують.

— Скорочуються експлуатаційні витрати, пов'язані з ідентифікацією та санацією некерованих і заражених систем, що не відповідають вимогам.

Як правило, система класу NAC складається з наступних компонентів:

— сервер контролю доступу;

— мережеві пристрої, які беруть участь в ідентифікації користувачів і застосуванні політик доступу;

— клієнт контролю доступу.

Слід зазначити, що раніше на ринку були представлені рішення двох класів – системи контролю доступу в мережу і системи централізованої аутентифікації, авторизації та розрахунків. Сьогодні провідні виробники систем інформаційної безпеки інтегрували функції обох класів систем в системи класу NAC.

Після впровадження NAC при кожній спробі кінцевого пристрою з'єднатися з мережею пристрій мережевого доступу (LAN, WAN, бездротового або віддаленого доступу) автоматично запитує профіль безпеки кінцевого пристрою, який видається за допомогою інстальованого клієнта або інструментів експертної оцінки. Потім ця профільна інформація зіставляється з мережевою політикою безпеки, і рівень відповідності пристрою цим політикам визначає реакцію мережі на запит доступу. Мережа може просто дозволяти доступ або відмовляти в ньому або ж обмежувати доступ, переадресуючи пристрій в сегмент мережі, в якому обмежений контакт з потенційно уразливими вузлами. Пристрій, що не відповідає вимогам, також можна помістити в карантин шляхом переадресації на коригувальний сервер, де в нього будуть внесені оновлення, які забезпечать дотримання політик. [11]

Зокрема, NAC може виконувати наступні перевірки дотримання політики безпеки:

— Чи працює на пристрої авторизована версія операційної системи.

— Чи внесені в ОС належні програмні виправлення або чи отримані останні оновлення.

— Чи інстальовано на пристрої антивірусне програмне забезпечення і чи є новітній набір файлів сигнатур.

— Чи активовані антивірусні ресурси.

— Чи інстальовані і чи правильно сконфігуровані персональний міжмережевий екран, інструменти запобігання вторгнень або інше програмне забезпечення безпеки ПК.

— Чи вносилися зміни чи несанкціоновані зміни в корпоративний образ пристрою.

Відповіді на ці та аналогічні питання, пов'язані з профілем безпеки, потім використовуються для винесення логічно-обґрунтованих, заснованих на політиці рішень щодо доступу в мережу.

2.2.3 Безпека бездротової точки доступу

Корпоративний Wi-Fi – це комплекс технічних рішень і продуктів, що працюють як разом, так і окремо, де кожен бере на себе навантаження і виконує свою частину роботи. У сукупності складається одна велика система, покликана допомогти, спростити і вирішити весь спектр завдань, що виникають сьогодні стосовно до мережі Wi-Fi.

Стандарти безпеки, які застосовувалися спочатку в бездротових мережах (IEEE 802.11, WEP), мали певні недоліки. Метод захисту полягав у використанні ідентифікаторів мережі SSID (Service Set Identifier), аутентифікації за MAC-адресою і відкритої аутентифікації із загальним ключем по протоколу WEP (Wired Equivalent Privacy). Протокол WEP застосовує статичні ключі, алгоритм шифрування RC4, а також не вимагає обов'язкової аутентифікації користувача і легко розкривається. Дані методи застосовуються і на сьогоднішній день, але є застарілими і не відповідають вимогам щодо забезпечення належного рівня безпеки в організації.

Тим не менш існує надійне рішення щодо захисту точок доступу на канальному рівні на базі протоколів EAP (Extensible Authentication Protocol), TKIP (Temporal Key Integrity Protocol) і алгоритму шифрування AES. Протокол EAP підтримує надійні схеми аутентифікації з використанням Radius-сервера, динамічні сесійні ключі і алгоритми управління ключами. Перераховані технології є компонентами нових стандартів з безпеки бездротового доступу IEEE 802.11 і і WPA / WPA2 (Wi-Fi Protected Access) і забезпечують надійний спосіб взаємної і централізованої (за допомогою Radius-сервера) аутентифікації і шифрування (рис 2.8). [5]

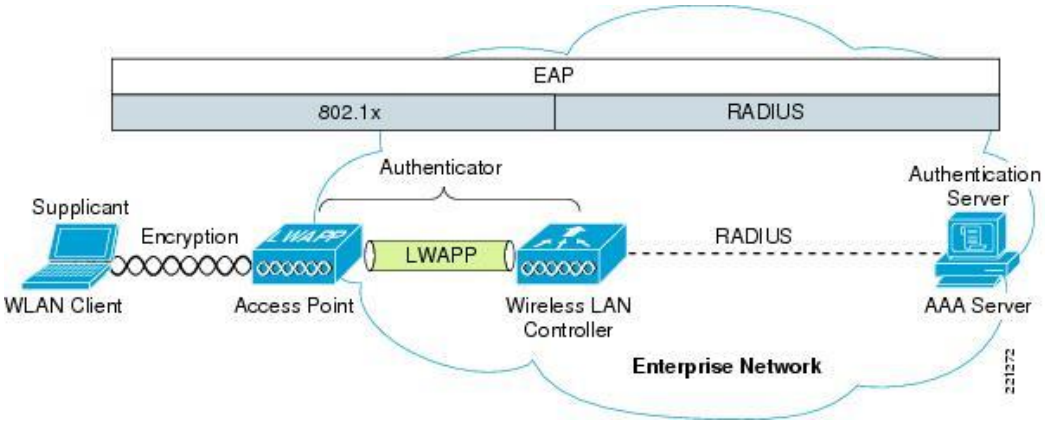

Рисунок 2.8 - Приклад забезпечення безпечного підключення до бездротової корпоративної мережі

Для захисту точок доступу висуваються наступні основні вимоги:

— Передані дані в бездротовій мережі повинні бути захищені за допомогою надійних механізмів забезпечення конфіденційності даних, що використовують безпечні протоколи (наприклад, EAP, TKIP, AES).

— Устаткування бездротової мережі повинно надавати можливість:

  — регулювання рівня потужності переданого радіосигналу;

  — підтримки подачі живлення по Ethernet -кабелю;

  — формування декількох бездротових мереж на одній точці доступу з різним рівнем безпеки;

- підтримки механізмів безпеки: Wireless Protected Access (WPA), 802.11i;
- підтримки механізмів виявлення несанкціонованих точок доступу, тимчасових бездротових мереж, джерел перешкод;
- швидкого роумінгу (обладнання бездротової мережі повинно забезпечувати перемикання між точками доступу не більше ніж за 50 мс).

Дані протоколи і вимоги підтримують точки доступу різних компаній, таких, як Cisco Aironet , Zyxel , D-Link і ін.

Основними компонентами рішення є:

- точка радіодоступу;
- комутатор доступу;
- DHCP-сервер (сервер Active Directory);
- сервер контролю доступу (Radius-сервер); бездротовий адаптер Wi-Fi на комп'ютері користувача.
- технологія VPN

Іншим кардинальним способом забезпечення безпеки для бездротових мереж є технологія VPN, яка забезпечує шифрування (конфіденційність), електронний цифровий підпис (цілісність, імітостійкість, аутентифікацію) на мережевому рівні. VPN-шлюзи дозволяють здійснити захищений доступ віддалених абонентів до ресурсів корпоративної мережі. Дана технологія може використовуватися для посилення заходів захисту, описаних раніше.

2.3 Хмарні технології захисту

2.3.1 Software as a service (SaaS)

Software as a service (SaaS) («Програмне забезпечення як послуга») – модель ПЗ, при якій постачальник ПЗ розробляє додаток і самотужки керує

ним, надаючи замовникам доступ через інтернет (рис 2.9). Одною з переваг моделі SaaS для споживача є відсутність необхідності установки, підтримки і оновлення ПЗ.

SaaS – це тип хмарних обчислень пов'язаний з іншими категоріями хмарних обчислень: інфраструктура як послуга IaaS (Infrastructure as a Service) і платформа як послуга PaaS (Platform as a Service).

Користуючись моделлю SaaS, замовники платять не за володіння програмним забезпеченням, а за його оренду (тобто, його використання через веб-інтерфейс). Тому, на відміну від звичайної схеми ліцензування програмного забезпечення, замовник несе відносно невеликі періодичні витрати. Немає необхідності інвестувати кошти для придбання програмного забезпечення та його підтримки. Схема періодичної оплати передбачає, що в разі, якщо необхідність в програмному забезпеченні тимчасово відсутня, можна призупинити його використання та не виплачувати кошти розробнику.

З точки зору розробника, модель SaaS дозволяє ефективно боротися з не ліцензійним використанням програмного забезпечення (піратством). Окрім цього, SaaS дозволяє значно зменшити витрати на розгортання і впровадження інформаційних систем, хоча і не виключає їх повністю. [12]

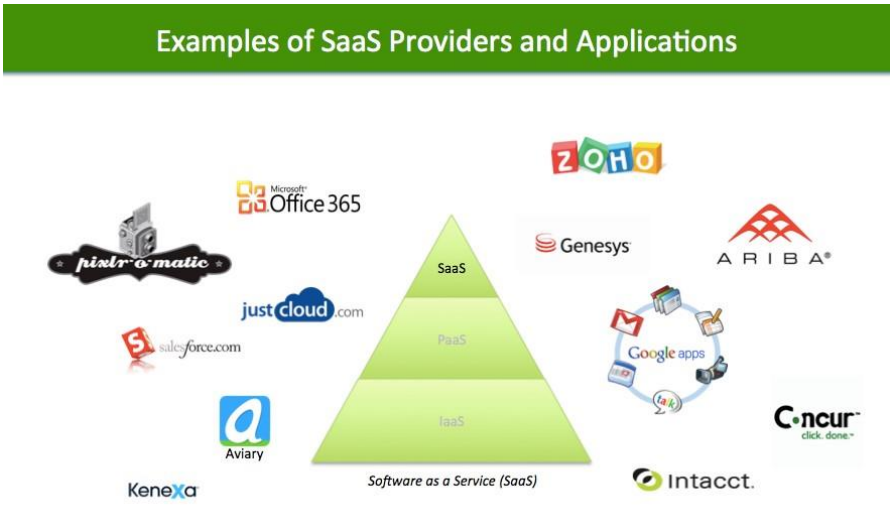

Рисунок 2.9 - Приклади компаній та програм, що пропонують SaaS послуги

Переваги SaaS:

— Оновлення. Програмне забезпечення, розміщене на сервері, може оновлюватися централізовано, на відміну від традиційної моделі, в якій програмне забезпечення необхідно буде оновлювати на кожній машині. Іншими словами, SaaS можна легко підтримувати за допомогою останньої версії програмного забезпечення в будь-який час.

— Апаратне забезпечення. За допомогою програмного забезпечення, що запускається на сервері, окремі ПК не потрібно оновлювати відповідно до вимог обладнання і немає проблем з недотриманням мінімальних вимог.

— Витрати. При використанні моделі підписки, (авансові) витрати на придбання знижуються для підприємств. Крім того, користувачі можуть додаватися по мірі необхідності щомісяця, щоб бізнес міг розширюватися в міру необхідності.

— Швидке розгортання. Оскільки програмне забезпечення не потрібно встановлювати і налаштовувати на окремих комп'ютерах, з SaaS його можна розгортати набагато швидше.

— Доступність. Для отримання доступу до додатка SaaS потрібно тільки браузер і підключення до Інтернету, що дозволяє користувачам входити в систему з будь-якого місця. Крім того, дані користувача зберігаються в хмарі і не прив'язані до ПК окремого користувача, що полегшує співпрацю з іншими користувачами.

Недоліки SaaS:

— Необхідність інтернету. Щоб використати SaaS користувач повинен бути підключений до інтернету. Для тих випадків, коли користувачі відключені, наприклад, під час подорожі на літаку (хоча в наші дні все більше пропонують Wi-Fi в польоті), або якщо інтернет відключається в службових приміщеннях, SaaS буде недоступний.

— Повільна робота. Залежно від швидкості вашого інтернет-з'єднання та інших необхідних ресурсів, SaaS-пропозиція може працювати повільніше, ніж якби програмне забезпечення працювало локально.

2.3.2 Platform as a system (PaaS)

PaaS – це комплект сервісів для створення сучасних додатків локально і в хмарі, а також для управління ними (рис 2.10).

PaaS надає інфраструктуру і ПО середнього шару, що дає можливість розробникам, IT-адміністраторам і кінцевим користувачам створювати, інтегрувати, переносити, розгортати мобільні і веб-додатки, а також забезпечувати їх безпеку і керованість.

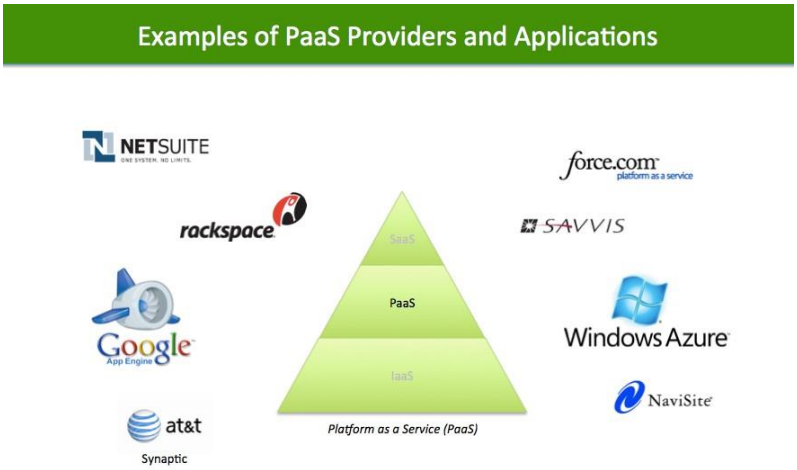

Рисунок 2.10 - Провайдери послуг PaaS

Для підвищення продуктивності PaaS пропонує готові програмні компоненти, які дають можливість розробникам додавати в додатки нові функції, включаючи такі передові технології, як штучний інтелект, чат-боти, блокчейн та Інтернет речей (IoT). Сюди також включаються набори інструментів розробки додатків, в тому числі власні хмарні сервіси, Kubernete, Docker і container engines, а також багато інших.

Сервіси PaaS також включають в себе рішення для аналітиків, кінцевих користувачів і адміністраторів IT, в тому числі для аналізу великих даних, управління змістом, управління даними і базами даних, системного управління та забезпечення безпеки в хмарі.

Послуги PaaS можуть доставлятися через публічне, приватне або гібридне хмарне середовище.

У публічному типу хмари PaaS клієнт контролює запуск ПЗ, а хмарний провайдер надає йому компоненти для цього – сервери, сховище, мережу, ОС і бази даних.

У приватній хмарі модель PaaS працює як ПЗ або устаткування всередині брандмауера клієнта, зазвичай в його датацентрі. Гібридна хмара моделі PaaS надає змішані послуги двох видів хмари: приватного і публічного. Замість того, щоб надати компанії цілу IT-інфраструктуру для розробки ПЗ, модель PaaS надає ключові послуги, такі як хостинг додатків або розробку Java.

Деякі послуги PaaS включають дизайн, розробку, тестування і запуск додатків. Послуги PaaS також можуть включати інтеграцію веб-сервісів, співпрацю з командою розробників, інтеграцію баз даних і захист даних.

Як і з іншими типами хмари, клієнти платять за PaaS за фактом використання. Деякі провайдери знімають фіксовану місячну плату за доступ до платформи і додатків, розміщених на ній.

PaaS володіє всіма основними перевагами хмарних обчислень: від прозорого ціноутворення і простого виділення ресурсів до масштабування на вимогу і аварійного відновлення. Управління здійснюється за допомогою уніфікованих панелей. [12]

Задачі, для яких використовується PaaS:

— Розробка і управління API. Компанії використовують PaaS, щоб розробляти, запускати, управляти API і мікросервісами. Це включає створення нових API і інтерфейсів для існуючих API.

— Бізнес-аналіз. Інструменти, які надаються по PaaS, дозволяють компаніям аналізувати дані. За допомогою них компанії знаходять інсайти для бізнесу і моделей поведінки, які допомагають їм приймати кращі рішення і точніше прогнозувати події, наприклад, попит на ринку.

— Керування бізнесом. Компанії можуть використовувати PaaS, щоб отримати доступ до платформи управління бізнесом. Платформа управління надається як сервіс нарівні з іншими хмарними послугами.

— Комунікація. Модель PaaS може також служити механізмом доставки для платформ комунікації. Це дозволяє розробникам додавати опції спілкування: голос, відео, месенджери.

— Бази даних. Провайдер PaaS може надавати такі послуги, як встановлення та підтримку баз даних компанії.

— Інтернет речей. У PaaS підтримуються середовища додатків, мови програмування і інструменти, які використовуються для інтернету речей.

— Управління майстер-даними. В управління майстер-даними входять процеси, політики, стандарти і інструменти, які керують важливими бізнес-даними компанії. Такі дані можуть включати інформацію про транзакції клієнтів, аналітику.

2.3.3 Інфраструктура як послуга (IaaS)

Інфраструктура як послуга (англ. Infrastructure as a Service; IaaS) – одна з моделей обслуговування в хмарних обчисленнях, за якою споживачам надаються за передплатою фундаментальні інформаційно-технологічні ресурси – віртуальні сервери із заданою обчислювальною потужністю, операційною системою (найчастіше – встановленою провайдером з шаблону) і доступом до мережі (рис 2.11).

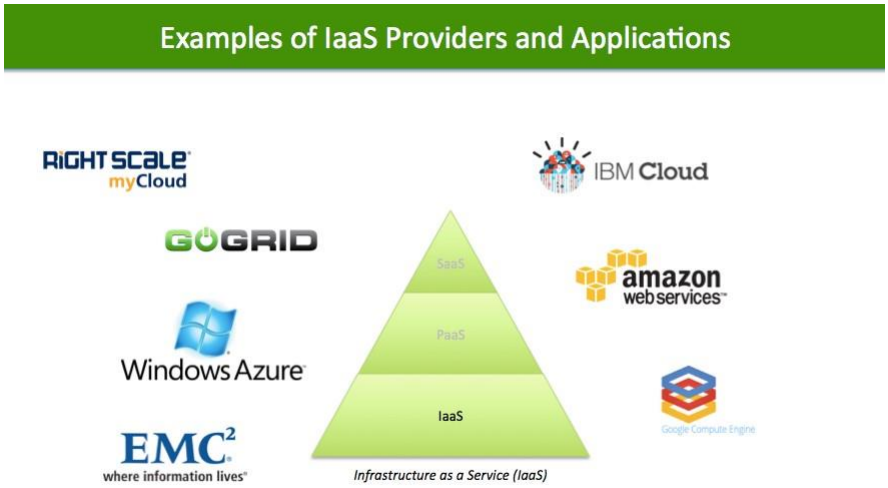

Рисунок 2.11 - Компанії, що надають послуги IaaS

При підписці за моделлю «інфраструктура як послуга» споживач, як правило, здобуває серверний час, помножений на кількість задіяних віртуальних процесорів і віртуальних обсягів пам'яті, а також простір зберігання (можливо, з різною тарифікацією в залежності від продуктивності), задану мережеву пропускну здатність, в деяких випадках – мережевий трафік.

IaaS знаходиться на найнижчому рівні серед хмарних моделей обслуговування. На відміну від моделі PaaS (де провайдер надає готове програмне забезпечення, СУБД, засоби розробки) і SaaS (на якому надається прикладне програмне забезпечення), в IaaS не передбачено контроль з боку постачальника послуг за тим, яке встановлюється програмне забезпечення, він контролює лише фізичну і віртуальну інфраструктуру.

Інфраструктура як послуга (IaaS) – це служба хмарних обчислень, де підприємства орендують сервери для обчислень і зберігання в хмарі. Користувачі можуть запускати будь-яку операційну систему або додатки на орендованих серверах без витрат на обслуговування і експлуатацію цих серверів. Інші переваги інфраструктури як послуги включають надання клієнтам доступу до серверів в географічних точках, близьких до їх кінцевих користувачів. IaaS автоматично масштабується як вгору, так і вниз, в

залежності від попиту, і забезпечує гарантовану угоду про рівень обслуговування (SLA) як з точки зору часу безвідмовної роботи, так і продуктивності. Це усуває необхідність вручну виділяти і управляти фізичними серверами в центрах обробки даних.

Інфраструктура як послуга (IaaS) може бути більш ефективною для підприємства, ніж володіння і управління власною інфраструктурою. Нові додатки можна тестувати з постачальником IaaS замість придбання інфраструктури для тестування. [12]

Інші переваги інфраструктури як послуги включають в себе:

— Безперервність і відновлення після збою. Хмарна служба в різних місцях забезпечує доступ до програм та даних під час аварії або простою.

— Прискорене масштабування – швидке збільшення і зменшення ресурсів відповідно до вимог додатків у всіх категоріях хмарних обчислень.

— IaaS дозволяє підприємствам більше зосередитися на основній діяльності, а не на IT-інфраструктурі і обчислювальних ресурсах.

Реалізація IaaS може бути в публічному, приватному або гібридному хмарному середовищі (рис 2.12). Клієнти використовують графічний інтерфейс для зміни інфраструктури в міру необхідності. До інфраструктури також можна отримати доступ через ключ API, тому нові сервери включаються в роботу автоматизовано, коли це необхідно.

Рисунок 2.12 - Порівняння публічного та приватного середовища

Підприємства використовують IaaS для більш ефективного виконання наступних завдань:

— Тестування та розробка. Середовища тестування і розробки швидко і легко налаштовуються за допомогою IaaS. Це дозволяє швидше виводити додатки на ринок.

— Створення резервних копій та відновлення. IaaS вирішує проблеми управління зберіганням і відновлення. Він обробляє непередбачувані потреби і потреби в зберіганні без необхідності виділяти персонал для управління ними.

— Аналіз великих даних. IaaS забезпечує обчислювальну потужність для економічного видобутку великих масивів даних.

Користувачі IaaS користуються багатьма перевагами інфраструктури як послуги, такими як доступ до тих же сервісів технології інфраструктури традиційного центру обробки даних без необхідності інвестувати стільки ресурсів. Це гнучка модель хмарних обчислень, яка дозволяє автоматизувати розгортання серверів, обчислювальної потужності, сховища і мереж.

2.3.4 Security as a Service (SecaaS)

Безпека як послуга, або Security as a Service (SecaaS) – це бізнес-модель, в якій провайдер послуг безпеки інтегрує свої сервіси в корпоративну інфраструктуру замовника. При цьому сукупна вартість володіння для компанії знижується за рахунок хмарної архітектури рішень, оплати сервісів по підписці і відсутності капітальних витрат для замовника.

Деякі категорії SecaaS – антивірусна і антиспам-фільтрація електронної пошти в хмарі, сервіси по захисту від DDoS-атаки. Все більше підсистем безпеки йдуть в хмару, так як це дозволяє захищати дані в нових IT-системах і пристосовуватися до мінливої IT-інфраструктури.

SecaaS-рішення, що базуються на хмарних технологіях, на відміну від традиційних засобів захисту (on-premise), архітектурно краще підходять для захисту даних в новій IT-інфраструктурі, до якої відносяться:

— Мобільні співробітники з ноутбуками, смартфонами і планшетами. Приклад – традиційні засоби контролю веб-доступу і URL-фільтрації, що встановлюються всередині периметра компанії, що не здатні захищати доступ віддалених співробітників. SaaS-рішення для веб-фільтрації, що використовує найближчий до користувача сервер фільтрації і агентів захисту на ноутбуках і мобільних пристроях, вирішує цю задачу.

— Динамічна і масштабована інфраструктура веб-додатків. Приклад: традиційний Web Application Firewall (WAF), що встановлюється всередині периметра, не зможе захистити веб-додаток, динамічно розгорнутий в декількох дата-центрах. Неможливо перенести вже куплений WAF в хмару Amazon або Azure. Не можна налаштувати WAF на роботу з декількома резервними дата-центрами для обробки трафіку одного веб-додатку, якщо, звичайно, компанія не придбає кілька WAF, що неодмінно збільшить TCO(total cost of ownership). Хмарний Web Application Firewall, що надається по SaaS-моделі, здатний економічно ефективно впоратися із завданням захисту веб-додатків в сучасних інфраструктурах.

— Хмарні сервери, інфраструктура як сервіс (IaaS), гібридні хмари. Для прикладу візьмемо базові підсистеми безпеки – міжмережеве екранування і виявлення вторгнень. У традиційній корпоративної інфраструктурі ці підсистеми безпеки реалізуються на апаратних платформах. Але для серверів в публічній або гібридній IaaS інфраструктурі необхідні більш гнучкі. Найбільшу цінність і зручність керування надають SecaaS-рішення, які інтегруються з інтерфейсами управління IaaS-платформи.

Рішення ІБ, спроектовані для роботи за моделлю SaaS, дозволяють компаніям отримати більш актуальний захист у порівнянні з on-premise-системами за рахунок декількох факторів:

— Використання великого обсягу даних для ІБ-аналітики – чим більше клієнтів використовує рішення, тим більше сигнатур, інформації про атаки і загрози та інших індикаторів компрометації отримують розробники і користувачі системи. Наприклад, розподілена SaaS-система захисту від DDoS-атаки, виявивши паразитний трафік, може автоматично заблокувати такий трафік від відомого шкідливого джерела у всіх клієнтів. Ключовим моментом є швидкість поширення таких даних.

— Моментальні і постійні оновлення – вся інформація про атаки і загрози може оновлюватися в реальному часі в централізованому ядрі SaaS-продукту. Таким чином, один раз виявивши, наприклад, центр управління ботнетом, система безпеки може відразу заблокувати трафік до такого серверу на всіх машинах, що необхідно захистити.

— Швидке впровадження і можливість оперативної заміни рішення. Компанія може отримувати передові технології, адже термін впровадження рішення істотно нижче, а схема pay-as-you-go дозволяє швидко змінити постачальника. Проста зміна SecaaS-провайдера дає можливість отримувати кращі технології без прив'язки до термінів амортизації обладнання. [13]

До SecaaS застосовні всі вигоди і переваги використання хмарних і SaaS-рішень, такі як:

— Динамічна масштабованість і практично необмежені доступні ресурси – хмарна архітектура рішень здатна масштабуватися на вимогу, наприклад, дозволяючи швидко підключати нові сервери, сайти, мобільні пристрої, що необхідно захистити.

— Гнучка система оплати за спожиті ресурси – pay-as-you-go, доступна в деяких хмарних рішеннях безпеки, наприклад, вартість системи захисту хмарних серверів може бути прив'язана до тривалості роботи самого сервера, що захищається, тобто компанія не оплачує даремно захист вимкненого сервера, що досить часто можна зустріти в динамічно масштабованій IaaS-інфраструктурі.

— Швидкість впровадження та отримання результатів. Швидкий старт і оперативне підключення, оскільки немає необхідності готувати інфраструктуру всередині компанії. Це дозволяє швидше отримувати видимі результати.

2.4 Висновки до розділу 2

У розділі 2 розглянуті програмно-апаратні, мережеві та хмарні засоби захисту. Засоби захисту інформації - це лінійка пристроїв і пристосувань, приладів та технічних систем, а також інших виробів, що застосовуються для вирішення різних завдань із захисту інформації.

Програмно-апаратні засоби (брандмауер, служби фільтрування контенту, системи IDS та IPS, Honeypot) фільтрують та, якщо необхідно, блокують вхідний та вихідний несанкціонований трафік, виявляють та запобігають незаконним вторгненням до системи та відволікають зловмисників від реальних систем.

Мережні засоби захисту (технологія VPN, контроль мережевого доступу та безпека бездротової точки доступу) забезпечують захист всіх кінцевих пристроїв, що мають доступ до мережі від присутніх всередині загроз безпеки, створюють надійні зашифровані канали за допомогою таких технологій як VPN та контролюють безпечні бездротові з’єднання у інфраструктурі компанії.

Також проаналізовані переваги хмарних технологій захисту інформації (SaaS, PaaS, IaaS, Secaas). До них відносяться можливість завжди отримувати високотехнологічне та оновлене до останньої версії ПЗ, легкість налаштування та масштабування, швидкість відновлення після збоїв.

3 ВПРОВАДЖЕННЯ ОСВІТИ І НАВЧАННЯ В ГАЛУЗІ КІБЕРБЕЗПЕКИ

3.1 Важливість впровадження освіти і навчання в галузі кібербезпеки

Керівники підприємств розуміють важливість підвищення обізнаності співробітників з питань інформаційної безпеки.

Велика частина сучасних цифрових атак починається з атаки на людей. У хід йдуть психологічний вплив і соціальна інженерія, використання яких змушує жертв атаки виконати потрібну злочинцям дію: перейти за посиланням, відкрити вкладку або ввести дані від облікового запису на сайті шахраїв. Технічні засоби захисту майже завжди використовуються, але рідко допомагають вберегтись від таких атак.

Аргумент на користь навчання співробітників з питань кібербезпеки простий: якщо співробітники не знають, як розпізнати загрозу безпеці, як можна очікувати, що вони зможуть її уникнути, повідомити про неї або ліквідувати?

При цьому, у постраждалих компаній майже завжди є і брандмауери і захисне ПЗ. Тільки цього недостатньо. Працівники, а не технології, є найбільш вразливою ланкою перед атаками.

Це зовсім не означає, що співробітники, що попалися в пастку, є безвідповідальними. Вони роблять звичайні людські помилки – довіряють фальшивим особистостям, спокушаються наживкою, становляться жертвами інших тактик, використовуваних злочинцями для отримання доступу до інформації компанії. Це трапляється, якщо вони не підготовлені до подібних загроз і атак, не брали участі в тренінгах та навчальних програмах по кібербезпеці.

Щоб захистити себе і компанію від кібератак, співробітникам необхідно пройти навчання. Ознайомлення працівників із загрозами безпеці, порядком дій при виявленні загрози, сприяє зміцненню найбільш вразливої ланки ланцюжка бізнесу.

Сьогодні улюбленою тактикою кіберзлочинців є соціальна інженерія – психологічне маніпулювання жертвами з метою переконати їх добровільно чи несвідомо надавати приватні дані. Іншою технікою є фішинг – більшість кібератак на компанії є результатом фішингових шахрайств, тому навчання основам фішингу є необхідним.

Поряд з цими двома видами віртуального шахрайства, шкідливе ПЗ також являє собою постійну загрозу – це стосується завантаження додатків або програм, призначених для зламу пристроїв або надання доступу до мережі хакерам. [14]

Зміна моделей роботи та масштабне втручання інтернету в наше життя обумовлює необхідність навчання навичкам кібербезпеки співробітників.

3.1.1 Віддалена робота

У 2020 році через введення карантину для уникнення пандемії COVID - 19 віддалена робота стала новою реальністю для багатьох. Робота на дому поширилася до такої міри, що організації вибудовують окремі політики щодо дистанційних співробітників.

Дистанційна робота з використанням хмарних технологій підвищила рівень комфорту, але в той же час збільшила ризик вторгнень в організації. Співробітники несуть відповідальність за використання будь-яких персональних кінцевих пристроїв і повинні обмежувати використання службового обладнання корпоративними цілями. Проходження тренінгів з питань кібербезпеки навчає віддалених співробітників роботі з пристроями, коли вони знаходяться за межами інфраструктури підприємства.

3.1.2 Інтернет речей (IoT)

Співробітники підключають персональні пристрої до мереж компанії або навіть використовують їх для офіційної роботи. З'єднання персональних пристроїв з іншими машинами та мережами посилює їх вразливість.

Мобільні пристрої являють собою основну загрозу для внутрішньої IT - безпеки організації, оскільки більшість з них не мають відповідного захисту. З IoT - атаками можна впоратись, керуючи і, можливо, зводячи до мінімуму практику «принесених із собою пристроїв» на робоче місце, і забезпечуючи суворе дотримання політик безпеки серед співробітників.

3.1.3 Посилення державних регуляцій

Навчання і тренування з кібербезпеки більше не є особистим вибором. У багатьох державних нормативних актах, що підкреслюють політику безпечного використання комп'ютерів і мереж, програма підвищення обізнаності співробітників отримала вирішальне значення. Державні установи та законодавці підкреслюють важливість захисту підприємствами своїх IT-активів і цифрової інформації.

Всі співробітники компанії мають підвищити кваліфікацію з питань кібербезпеки. Працівники – це перша і основна лінія захисту від інтернет-злочинів. Будь-який співробітник, який має доступ до робочого комп'ютера або мобільного пристрою, повинен пройти тренінги з питань кібербезпеки. Адже практично кожен може стати мішенню. На персональних телефонах можуть зберігатися дані, які можна використовувати для доступу до корпоративних мереж; або, якщо співробітник стає жертвою крадіжки особистих даних, ця унікальна інформація може бути використана для створення помилкових профілів, які посилаються на бренд компанії, дозволяючи здійснювати шахрайства.

3.1.4 Теми, що слід включити в навчання

Щоб співробітники могли виявляти та запобігати порушенням, їм необхідне базові знання про різні форми загроз: спам, фішинг, шкідливі програми і програми-вимагачі, соціальну інженерію.

Матеріали по виявленню спаму повинні пояснити, що спам зустрічається не тільки в електронній пошті, але і в повідомленнях і запрошеннях в соціальних мережах. Наприклад, «запрошення до підключення» в LinkedIn може містити вірус.

Розповіді про фішинг повинні супроводжуватися прикладами реальних фішингових шахрайств, допомагаючи співробітникам зрозуміти, як виглядає фальсифіковане електронне повідомлення, від кого воно може прийти і яку інформацію може запросити.

Навчання повинно включати поради, що виключають завантаження шкідливого ПЗ або програм-вимагачів.

І, звичайно, обов'язковою темою повинна бути соціальна інженерія. Соціальні інженери маскуються під підроблені, але довірені особи в мережі і виманюють потрібну їм інформацію.

3.1.5 Важливість паролів

Сьогодні паролі потрібні скрізь – для розблокування своїх пристроїв, для входу в облікові записи і для кожної програми, пов'язаної з роботою. Як засіб безпеки, ця тактика призвела до того, що багато людей встановлюють загальні, повторювані паролі, які легко запам'ятати, і, відповідно, легко розгадати. Навчання кібербезпеці має допомогти зрозуміти, наскільки важливі паролі, розповісти про надійні програми, які можуть генерувати і зберігати паролі.

3.1.6 Політика щодо електронної пошти, інтернету і соціальних мереж

Звички поведінки співробітників з електронною поштою і соцмережами можуть поставити компанію під удар шкідливих програм, що атакують корпоративні програми та соціальні рахунки, що крадуть інформацію і гроші. Тому дуже важливо, щоб тренінги включали в себе політику та рекомендації щодо використання електронної пошти, Інтернету і соціальних мереж.

3.1.7 Захист даних компанії

У кожної компанії є власна політика захисту даних, але не варто припускати, що всі співробітники знають про цю політику, або що вони її розуміють. Тренінги з інформаційної безпеки для нових співробітників повинні пояснювати нормативні та правові зобов'язання захисту даних. Не варто забувати і про регулярні курси підвищення кваліфікації, щоб всі співробітники пам'ятали правила і знали, коли вони змінюються.

3.1.8 Виявлення і повідомлення про загрози кібербезпеки

Кожен пристрій, який використовують співробітники та електронна пошта, яку вони отримують і відкривають, може містити підказки про те, що там ховається вірус, фішингове шахрайство або злом пароля. Але щоб по-справжньому мобілізуватися проти атак, тренінги повинні допомогти співробітникам дізнатися про непояснені, на перший погляд, помилки, спам і антивірусні попередження. І обов'язково необхідно навчити співробітників тому, кому і як слід повідомляти про підозрілі дії.

3.1.9 Методи навчання

При навчанні персоналу краще не погоджуватися на будь-які готові навчальні модулі або базові веб-курси. Більш розумно вкладати кошти в професійних експертів з кібербезпеки, які будуть працювати безпосередньо з організацією. Таке спеціалізоване навчання дозволяє розробити повноцінну віртуальну стратегію захисту, що враховує унікальну корпоративну структуру, ступінь конфіденційності даних і потреби співробітників.

Метою такого навчання завжди є зміна звичок і поведінки щодо безпеки, створення почуття загальної відповідальності. Неважко зрозуміти, що одноразового інформування по вищепереліченим темам недостатньо для досягнення цієї мети. Тренінги з кібербезпеки варто проводити часто, надаючи можливості практикувати безпечну онлайн-поведінку в проміжках між заняттями.

2.2 Створення культури обізнаності про кібербезпеку

Звичайно, зусилля в першу чергу спрямовані на формування знань в сфері кібербезпеки, саме знання її основних правил і дотримання їх щодня в своїй діяльності на рівні звички стають умовою успішної протидії кіберзлочинцям. Але неможливо прищепити стійкі знання і сформувати правила, яким співробітник буде слідувати в своєму повсякденному житті, якщо у нього немає розуміння, для чого йому ці знання необхідні, якщо суспільство не поділяє їх цінність і дотримання ним нетипово для середовища, в якому людина живе. Тому важливо не тільки підвищувати обізнаність, а й формувати культуру кібербезпеки, що складається з безлічі елементів.

Крок за кроком, шляхом «нанизування» одного елемента на інший, відбувається формування культури, що вимагає залучення значних ресурсів, в тому числі тимчасових. Тим не менш необхідно вибрати саме такий шлях,

оскільки формування культури кібербезпеки – найбільш ефективний проактивний метод протидії кіберзлочинності, спрямованої на «злам» людини.

Сьогодні найбільші цифрові компанії вносять свій внесок у формування культури кібербезпеки, інтегруючи її в свою корпоративну культуру. Наприклад, цінність «Я - Лідер» передбачає відповідальність кожного співробітника за себе і за те, що відбувається навколо. Звідси випливає відповідальне і усвідомлене ставлення співробітників до підвищення власної кіберграмотності.

Рік від року зростає кіберзлочинність, кіберзлочинці шукають «слабку ланку» в компанії, через яку можуть отримати доступ до її систем. І найчастіше такою ланкою виявляється людина. Саме тому високий рівень культури кібербезпеки співробітників має величезне значення. Необхідно вести планомірну роботу по формуванню культури кібербезпеки як сукупності елементів, що створюють основу ефективного поширення знань, формування звички керуватися правилами кібербезпеки в житті.

Важливу роль для компанії, яка веде бізнес в цифровому середовищі, що охоплює мільйони клієнтів, має безпека клієнтів, але кожен з них, на жаль, може зіткнутися з кібершахрайством. Тому, щоб допомогти клієнтам підвищити обізнаність в області кібербезпеки і поліпшити навички безпечної роботи в кіберсередовищі, важливо на регулярній основі навчати клієнтів і допомагати їм виробляти і розвивати навички кібербезпеки.

Усвідомлена участь клієнтів компанії у власному кіберзахисті – необхідна умова успіху розвитку бізнесу, тим більше, коли мова йде про сучасні цифрові компанії, що активно впроваджують новітні технології. Компанії повинні докласти максимум зусиль, щоб допомогти засвоїти клієнту цю нову звичку.

Раніше було зазначено, що для ефективного створення знань важливо будувати культуру кібербезпеки, що складається з безлічі елементів, що формують сприятливе середовище для поширення і розвитку цих знань.

Традиції, цінності, мова, символи, правила – ті основні елементи культури, чиє формування дозволяє підвищувати ефективність заходів, спрямованих на поширення цих знань.

Будь-яка культура ґрунтується на традиціях – елементах соціальної і культурної спадщини, що зберігаються в певному співтоваристві. Традиції є необхідною умовою його життєдіяльності і передаються з покоління в покоління. Такі традиції, як прочитання раз в тиждень інформаційного дайджесту з кібербезпеки, занурення в інформаційне поле кібербезпеки, аналіз проблем та досягнень на щорічній сесії кібербезпеки, об'єднують співробітників і мотивують до розвитку знань.

Соціально значущі цінності – це відповіді на питання, чому і навіщо потрібно кожному з нас сьогодні підвищувати свою кіберграмотність, а правила регулюють поведінку відповідно до цих цінностей. Загальнокультурна цінність – безпека, деталізується в таких напрямах, як професіоналізм, постійний розвиток своїх компетенцій, дотримання правил кібербезпеки в повсякденному житті, навчання правилам кібербезпеки інших і, звичайно ж, дотримання правил і стандартів безпеки своєї організації.

Слід приділяти велику увагу просвітницькій роботі в області кібербезпеки: доповіді та статті співробітників служб кібербезпеки, залучення всіх співробітників в інтерактивні ігри та квести – ці зусилля дають свої плоди.

Мова – знакова система, яка використовується в конкретному соціумі. Мова виконує функції створення, зберігання та передачі інформації. Як це не дивно прозвучить в століття технологій, які дають нам безліч каналів для зв'язку, компанії, особливо великі, стикаються з проблемою комунікацій. І дуже часто подія обертається інцидентом тому, що фахівцям не вдалося зрозуміти один одного або вчасно не вдалося знайти людину, якій можна задати питання і, отримавши консультацію, виконати грамотні дії.

Рішенням є створення єдиної точки входу, куди можна звернутися з будь-якого питання кібербезпеки і отримати компетентну оперативну

відповідь. Наприклад, створення центру підтримки кібербезпеки – гарячої лінії, по якій будь-який співробітник, з одного боку, може вирішити виниклу у нього проблему і захистити себе, а з іншого – допомогти службі кібербезпеки запобігти інциденту на стадії його зародження і тим самим захистити компанію.

Знаки відмінності – один з найдавніших артефактів. Ще в давні часи існували особливі символи, що дозволяють відрізнити членів одного роду від іншого. Знаки відмінності надавали підтримку і виступали об'єднуючим початком. Таким об'єднуючим початком може стати логотип. Використання логотипу в комунікаціях, матеріалах визначає високий контроль якості, єдину мову, вивірену термінологію. Застосування брендової продукції вказує на приналежність до команди.

Єдине поле комунікації, відчуття співробітником частиною команди, що розділяє спільні традиції і цінності, – основа, яка формує ефективне підвищення обізнаності, безперервне навчання працівників та клієнтів.

3.3 Висновок до розділу 3

У третьому розділі розглянуто питання навчання робітників організацій навичкам кібербезпеки. Зазначено, що велика кількість цифрових атак на компанію здійснюються за допомогою соціальної інженерії, де у хід йде психологічний вплив та різні засоби маніпулювання. Найчастіше технічні засоби не можуть допомогти уникнути таких загроз. Саме тому необхідне навчання співробітників. Навчання допоможе співробітникам виявити додатки з шкідливим ПЗ, фішинг, спам та не стати жертвами маніпуляцій, дасть змогу вирішити інцидент одразу після його виникнення.

Важливим елементом є створення культури обізнаності у сфері кібербезпеки. Це стимулює робітників завжди покращувати свої навички та бути обізнаними у цій галузі.

4 ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1 Основні поняття політики безпеки

Політикою інформаційної безпеки (ІБ) називається комплекс заходів, правил і принципів, якими в своїй повсякденній практиці керуються співробітники підприємства з метою захисту інформаційних ресурсів.

За час, що минув з виникнення самого поняття ІБ, напрацьовано чимало подібних політик. В кожній компанії керівництво саме вирішує, яким чином і яку саме інформацію захищати, і створює відповідні політики. Політики зазвичай формалізуються: розробляється відповідний регламент. Співробітники підприємства зобов'язані дотримуватися цього документу.

Політика безпеки є обов'язковою складовою певних стандартів (місцевих або міжнародних). Необхідна відповідність конкретним вимогам, які зазвичай висувають зовнішні аудитори, що вивчають діяльність організації. Відсутність політики безпеки породжує негативні відгуки, а подібні оцінки негативно впливають на такі показники, як рейтинг, рівень надійності, інвестиційну привабливість тощо.

ІБ включає в себе також проблематику відносин із персоналом (співробітник може розглядатися не тільки як особа, що підлягає захисту, а й як об'єкт, від якого інформація повинна бути захищена), та інші аспекти і фактори, що виходять за рамки виключно захисту телекомунікаційної мережі та запобігання несанкціонованого доступу до неї.

Для створення ефективної системи інформаційної безпеки повинні бути розроблені:

— концепція інформаційної безпеки (визначає політику в цілому, її принципи та цілі);

— стандарти (правила і принципи захисту інформації по кожному конкретному напрямку);

— процедури (опис конкретних дій для захисту інформації при роботі з нею: персональних даних, порядку доступу до інформаційних носіїв, систем і ресурсів);

— інструкції (докладний опис того, що і як робити для організації інформаційного захисту та забезпечення наявних стандартів).

Всі вищезазначені документи повинні бути взаємопов'язані і не суперечити один одному.

Також для ефективної організації інформаційного захисту слід розробити аварійні плани. Вони необхідні на випадок відновлення інформаційних систем при виникненні форс-мажорних обставин: аварій, катастроф і т. д.

Потрібно зауважити, що концепція інформаційного захисту не тотожна стратегії. Перша – статична, в той час як друга – динамічна.

Основними розділами концепції безпеки є:

— визначення ІБ;

— структура безпеки;

— опис механізму контролю над безпекою;

— оцінка ризику;

— безпека інформації: принципи і стандарти;

— обов'язки і відповідальність кожного відділу, управління або департаменту в здійсненні захисту інформаційних носіїв і інших даних;

— посилання на інші нормативи про безпеку.

Крім цього не зайвим буде розділ, що описує основні критерії ефективності в сфері захисту важливої інформації. Індикатори ефективності захисту необхідні, перш за все, менеджменту. Вони дозволяють об'єктивно оцінити організацію безпеки, не заглиблюючись в технічні нюанси. Відповідальному за організацію безпеки також необхідно знати чіткі критерії оцінки ефективності ІБ, щоб розуміти, яким чином керівництво буде оцінювати його роботу. [15]

Політику безпеки треба формулювати з урахуванням двох основних аспектів:

— Цільова аудиторія, на яку розрахована вся інформація з безпеки – керівники середньої ланки і рядові співробітники не володіють специфічною термінологією, але повинні при ознайомленні з інструкціями зрозуміти і засвоїти надану інформацію.

— Інструкція повинна бути лаконічною і при цьому вміщувати всю необхідну інформацію.

Після того, як документація по інформаційній безпеці готова, необхідна планова організація роботи щодо її впровадження в повсякденну роботу. Для цього необхідно:

— ознайомити колектив із затвердженою політикою обробки інформації;

— знайомити з цією політикою обробки інформації всіх нових працівників (наприклад, проводити інформаційні семінари або курси, на яких надавати вичерпні роз'яснення);

— ретельно вивчити наявні бізнес-процеси заради виявлення та мінімізації ризиків;

— скласти докладні методичні та інформаційні матеріали, інструкції, що доповнюють політику обробки інформації (наприклад, правила надання доступу до роботи в Інтернеті, порядок входу в приміщення з обмеженим доступом, перелік інформаційних каналів, по яких можна передавати конфіденційні дані тощо);

— раз в три місяці переглядати і коригувати доступ до інформації, порядок роботи з нею, актуалізувати прийняту по ІБ документацію, постійно моніторити і вивчати існуючі загрози ІБ.

4.2 Спеціалізовані політики безпеки

Існує безліч спеціалізованих політик, що застосовуються великою кількістю компаній. Деякі політики можуть підходити для багатьох організацій, інші є унікальними для певних умов організації.

Враховуючи особливості спеціалізованих політик безпеки, можна виділити дві групи:

— політики, що ураховують велику кількість користувачів;

— політики, що пов'язані з конкретними технічними умовами.

До спеціалізованих політик, що ураховують значну кількість користувачів, відносяться:

— політика допустимого використання;

— політика віддаленого доступу до ІС;

— політика міжмережевої взаємодії;

— політика захисту паролів тощо.

До спеціалізованих політик, пов'язаних з конкретними технічними умовами, відносяться:

— політика по шифруванню і управлінню криптоключами;

— політика конфігурації міжмережевих екранів;

— політика безпеки віртуальних захищених мереж VPN.

Розглянемо детальніше деякі з ключових спеціалізованих політик.

4.2.1 Політика паролів

Політика паролів – це набір правил, спрямованих на підвищення безпеки комп'ютера шляхом заохочення користувачів до використання надійних паролів і їх правильного використання.

Для багатьох політик потрібна мінімальна довжина пароля. Вісім символів є типовим значенням, але не може бути відповідним. Довші паролі

зазвичай більш безпечні, але деякі системи встановлюють максимальну довжину для сумісності із застарілими системами.

Деякі політики пропонують або накладають вимоги на тип пароля, який користувач може вибрати, наприклад:

— використання букв верхнього та нижнього регістру;

— включення однієї або декількох цифр;

— включення спеціальних символів, таких як @, #, $;

— заборона слів, знайдених в чорному списку паролів;

— заборона слів, що містяться в особистій інформації користувача;

— заборона на використання назви компанії або абревіатури;

— заборона паролів, які збігаються з форматом дати, номерами машин, телефонними номерами або іншими поширеними значеннями.

Інші системи створюють пароль для користувачів або дозволяють користувачеві вибрати один з обмеженого числа варіантів.

Деякі політики вимагають, щоб користувач змінював пароль періодично, часто кожні 90 або 180 днів. Системи, що реалізують такі політики, іноді не дозволяють користувачам вибирати пароль занадто близький до попереднього.

Необхідний рівень надійності пароля залежить, серед іншого, від того, наскільки легко зловмисникові представити кілька припущень. Деякі системи обмежують кількість разів, коли користувач вводить невірний пароль, перш ніж буде накладена затримка або обліковий запис буде заморожений.

4.2.2 Політика допустимого використання ІС

Ця політика описує допустиме використання телекомунікаційного та комп'ютерного обладнання в інформаційній системі. Політика поширюється на постійних співробітників та на все обладнання, яке є власністю або орендовано організацією.

Згідно політиці наступна діяльність забороняється без будь-яких винятків:

— Порушення прав будь-якої особи або компанії, захищених авторськими правами, комерційною таємницею, патентом або іншої інтелектуальної власності.

— Неавторизоване копіювання матеріалів, захищених авторським правом.

— Розміщення шкідливих програм в мережі або на сервері (наприклад, вірусів, хробаків, троянських коней, поштових бомб тощо).

— Повідомлення пароля від облікового запису або використання облікового запису стороннім.

— Використання обладнання для отримання або поширення матеріалів, що порушують законодавство.

— Розміщення шахрайських пропозицій товарів або послуг з використанням облікового запису компанії.

— Створення уразливостей або переривання роботи мережі.

— Сканування портів або виявлення уразливостей.

— Будь-який вид мережевого моніторингу, при якому перехоплюються дані, які не адресовані відповідному вузлу, крім випадків коли це є частиною трудової діяльності.

— Обхід систем входу і безпеки будь-якого вузла, мережі або облікового запису.

— Навмисне припинення роботи користувачів інформаційної системи (наприклад, DOS-атака).

— Використання будь-якої програми / скрипта / команди, або розсилка будь-яких повідомлень з метою відключення термінальної сесії користувача.

— Надання інформації або переліку співробітників компанії особам за межами організації.

4.2.3 Політика управління віддаленим доступом до ІС

Політика визначає стандарти для підключення до мережі організації з будь-якого хоста. Ці стандарти мінімізують потенційний ризик, який може виникнути в результаті несанкціонованого використання ресурсів компанії. Збитки включають в себе втрату конфіденційної, важливої для компанії інформації, інтелектуальної власності, нанесення шкоди репутації, пошкодження критичних внутрішніх систем тощо.

Ця політика включає віддалений доступ реалізований за допомогою, Dialup модемів, Frame Relay, ISDN, DSL, VPN, SSH, бездротових точок доступу тощо.

Найкращий брандмауер на ринку не захистить компанію, якщо вона будете підтримувати безліч незахищених модемів і точок бездротового доступу, відкритих для зовнішнього світу, в межах офісу. Співробітники іноді підключають до своїх робочих станцій неавторизовані модеми, щоб уникнути офіційно санкціонованого механізму дозволу і спростити доступ до даних свого робочого столу. Якою б не була причина цих механізмів несанкціонованого доступу, організаціям необхідно ретельно контролювати використання модемів для забезпечення віддаленого доступу до її систем. Весь зовнішній доступ до мереж, систем і даних повинен здійснюватися через централізовано кероване, протестоване і санкціоноване рішення віддаленого доступу. Повинна існувати політика, яка забороняє будь-яке несанкціоноване проникнення у системи, і будь-які виявлені механізми такого роду повинні бути негайно вилучені.

Вимоги політики:

— Компанія повинна строго контролювати безпечний віддалений доступ до мереж. Необхідно забезпечувати контроль за допомогою аутентифікації з використанням одноразового пароля або відкритих / закритих ключів.

— Необхідно переконатися, що персональний комп'ютер або робоча станція, які віддалено підключені до корпоративної мережі, не підключені одночасно до будь-якої іншої мережі.

— Не можна використовувати сторонні облікові записи електронної пошти або інші зовнішні ресурси для ведення бізнесу компанії.

— Маршрутизатор, налаштований для доступу до мережі, повинен відповідати мінімальним вимогам аутентифікації CHAP.

— Переналаштування домашнього обладнання для роздільного тунелювання заборонена в будь-який час.

— Канали Frame Relay повинні відповідати мінімальним вимогам до аутентифікації стандартів DLCI .

— Нестандартні конфігурації обладнання повинні бути схвалені службами віддаленого доступу.

— Всі хости, що віддалено підключені до внутрішніх мереж, включаючи ПК, повинні використовувати останню версію антивірусного програмного забезпечення.

— Будь-яке особисте обладнання, яке використовується для підключення до мереж, має відповідати вимогам до обладнання віддаленого доступу.

— Організації або окремі особи, які бажають впровадити нестандартні рішення віддаленого доступу в виробничу мережу, повинні отримати попередній дозвіл від служб віддаленого доступу.

4.2.4 Політика міжмережевої взаємодії

Політика міжмережевої взаємодії визначає вимоги до безпеки інформаційного обміну організації із зовнішнім світом. Ця політика повинна відображати два аспекти:

— політику доступу до мережевих сервісів;

— політику роботи брандмауера.

Політика визначає правила надання та використання всіх можливих сервісів телекомунікаційної мережі. В рамках даної політики повинні бути задані всі сервіси і допустимі адреси для кожного сервісу. Крім того, для користувачів повинні бути вказані правила, що описують, коли і як користуватися сервісом і на якому комп'ютері це можна зробити.

Для того щоб міжмережевий екран вдало захищав ресурси компанії, політика повинна бути реалістичною. Реалістичною вважається така політика, за якої знайдений баланс між необхідним доступом користувачів до мережевих сервісів та захистом мережі організації від відомих ризиків.

Політика роботи брандмауера задає базовий принцип управління міжмережевою взаємодією. Вона кладеться в основу функціонування міжмережевого екрана. Може бути обраний один з двох принципів функціонування міжмережевого екрана:

— заборонено все, що не вказано у списку дозволеного;

— дозволено все, що не вказано у списку забороненого.

Фактично вибір принципу встановлює, наскільки «підозрілою» або «довірчою» повинна бути система захисту. Залежно від вибору, може бути прийнято рішення, як на користь безпеки в збиток зручності використання мережевих сервісів, так і навпаки.

4.2.5 Політика використання електронної пошти

Ця політика визначає стандарти обміну електронною поштою в інформаційній системі. Ці стандарти мінімізують можливе навантаження на інформаційну систему від несанкціонованих поштових повідомлень і вкладень. Загрози включають в себе втрату секретних і конфіденційних даних компанії або інтелектуальної власності, збиток репутації, пошкодження важливих систем і ненавмисне ознайомлення співробітника з приватною інформацією.

Згідно політики, забороняється:

— Відправлення несанкціонованих електронних повідомлень, включаючи розсилку спаму або інших рекламних матеріалів.

— Неавторизоване використання пошти або підробка заголовків повідомлень.

— Використання адреси, що не належить відправнику, з метою отримання відповідних повідомлень.

— Створення спам-розсилки з інформаційної системи компанії або інших систем з метою реклами послуг компанії

4.2.6 Політика шифрування

Ця політика спрямована на використання тільки тих алгоритмів шифрування, які довели свою ефективність.

Необхідно використовувати надійні стандартні алгоритми – DES3, Blowfish, RSA, RC5, AES, and IDEA в основі криптотехнологій. Ці алгоритми надають надійне шифрування, що використовується в сучасних додатках. Наприклад: PGP (Pretty Good Privacy) використовує комбінацію IDEA і RSA або алгоритм Діффі-Хелмана, а SSL (Secure Socket Layer) використовує просто RSA. Довжина ключа симетричних криптосистем повинна бути не менше 56 біт. Ключі асиметричних криптосистем повинні мати довжину, що забезпечує еквівалентну стійкість. Вимоги до довжини ключа повинні переглядатися щорічно і змінюватися з розвитком технологій.

Використання власних криптоалгоритмів в будь-яких цілях не допускається за винятком випадків, коли алгоритми перевірені незалежними експертами і затверджені.

4.2.7 Політика використання VPN

Призначення даної політики – визначення правил для VPN-підключень з використанням надійного шифрування при доступі до корпоративної мережі компанії.

Згідно політики, необхідно виконувати такі правила:

— Певні співробітники й авторизовані партнери можуть використовувати VPN. Користувачі VPN не повинні допускати несанкціонованого доступу інших користувачів до внутрішніх мережевих ресурсів компанії.

— Доступ по VPN повинен здійснюватися по одноразовому паролю за допомогою «токена» або за допомогою інфраструктури відкритих ключів зі стійкою фразою.

— Подвійне тунеллювання не допускається; дозволено тільки одне підключення до мережі.

— VPN-шлюзи налаштовуються і обслуговуються групою мережевої підтримки компанії.

— Всі комп'ютери, підключені до локальної мережі через VPN або за іншою технологією повинні використовувати найактуальніше стандартне антивірусне ПЗ.

— Користувачі VPN повинні автоматично вимикатися від локальної мережі після 30 хвилин простою. Користувач повинен авторизуватися заново, щоб підключитися до мережі. Команди ping або інша штучна мережева активність не повинні використовуватися для підтримки з'єднання.

— Користувачі комп'ютерів, котрі не належать компанії, повинні налаштувати своє обладнання у відповідності з політикою використання VPN і мережевих ресурсів.

— Використовуючи технологію VPN на особистому обладнанні користувачі повинні розуміти, що їхнє устаткування де-факто є частиною

мережі компанії і вони тим самим підкорюються тим же вимогам і правилам, що застосовуються до обладнання компанії, тому їх комп'ютери повинні бути налаштовані у відповідності з політиками безпеки.

4.3 Обробка інцидентів ІБ

Практика превентивних заходів у сфері інформаційної безпеки (ІБ) заснована на оцінці ризиків настання тієї чи іншої події інциденту ІБ. Фіксування факту настання події інциденту, очевидно, не може вважатися превентивним заходом, оскільки відображає факт, що вже відбувся інцидент. Першопричиною настання події інциденту ІБ є потенційна здатність зловмисника отримати необгрунтовані привілеї для доступу до активу організації. Оцінити ризик подібної можливості і прийняти правильне рішення про захист – основне завдання команди реагування.

Кожен ризик повинен бути оброблений відповідно до політики оцінки ризиків, прийнятої в організації. Оцінка ризиків розглядається як перманентний процес, метою якого є досягнення прийнятного рівня захисту. Іншими словами, повинні бути впроваджені достатні заходи захисту активу від необґрунтованого або неправомірного використання.

Для ефективної роботи команди реагування в організації повинні бути передбачені процедури, що забезпечують опис процесів функціонування підрозділів.

4.3.1 Виявлення та аналіз інцидентів ІБ

Домисел про інцидент ІБ у компанії, має опиратися такі характерні фактори:

— оповістка про інциденти ІБ прибувають водночас з декількох джерел (користувачі ІС, IDS, журнали подій);

— IDS сигналізують про множину повторюваних подій;

— аналіз лог-файлів неавтоматизованої системи дає підставу для висновку системним адміністратором про можливість настання події інциденту.

Ознаки інциденту можуть повідомляти, що інцидент відбувається саме в цей момент, і що інцидент, може статися в недалекому майбутньому. Далі представлені найчастіші ознаки події:

— IDS фіксує переповнення буфера;

— повідомлення антивірусної програми;

— крах Web -інтерфейсу;

— повідомлення користувачів про вкрай низьку швидкість при спробі виходу в Інтернет;

— фіксування системним адміністратором наявність файлів з нечитабельними назвами;

— повідомлення користувачів про наявність в своїх поштових скриньках безлічі повторюваних повідомлень;

— хост проводить запис в журнал аудиту про зміну конфігурації;

— додаток фіксує множинні невдалі спроби авторизації в файлі журналу подій тощо.

Приклади подій, які можуть служити джерелами повідомлень про інциденти ІБ:

— файли журналів подій сервера фіксують сканування портів ;

— оголошення в ЗМІ про появу нового виду експлойта тощо.

Після аналізу інциденту ІБ необхідно провести документації для збору і подальшої консолідації свідоцтв розслідування.

4.4 Процедури безпеки

Процедури безпеки – це докладні покрокові інструкції щодо того, як впровадити, увімкнути чи застосувати засоби контролю безпеки організації

згідно політики безпеки. Процедури безпеки повинні охоплювати безліч апаратних та програмних компонентів, що підтримують бізнес-процеси компанії, а також будь-які бізнес-процеси, пов'язані з безпекою (наприклад, приєднання нового працівника та призначення прав доступу).

Процедури покроково визначають, що треба зробити для:

— забезпечення швидкого реагування в критичних ситуаціях;

— реагування на конкретні події;

— усунення проблеми відмови в роботі.

Процедури безпеки спрямовують особу, яка виконує процедуру, до очікуваного результату.

Процедури безпеки ґрунтуються на політиці безпеки організації. Важливим принципом політики безпеки є те, що вона зосереджується на керівництві поведінкою. Як і політики безпеки, процедури безпеки також зосереджені на керівництві поведінкою. Політики безпеки стосуються того, хто, що і чому, а процедури безпеки інформують осіб в організації про те, коли (наприклад, щодня, щомісяця, за певним тригером), де і як.

Наприклад, підтримуюча процедура безпеки повинна визначати, коли виконуються резервні копії, до якого місця та середовища вони записуються, і як виконуються окремі кроки для її виконання.

Процедури безпеки повинні містити достатньо деталей, щоб їх можна було виконати. Політика безпеки окреслює потреби в безпеці загальним чином або на високому рівні. Процедури безпеки, навпаки, повинні надавати достатньо деталей, щоб особа, яка не знайома (або незначно знайома) з процесом або технологією, могла успішно досягти бажаного результату процедури. Необхідно уникати розробки процедур, які покладаються на знання експертів як основу для виконання процедури, оскільки це часто призводить до прогалин у процедурі. Хорошим тестом на рівень деталізації процедури є те, що хтось із молодших працівників виконує процедуру. Якщо вони можуть зробити це чисто, тоді, ймовірно, у процедурі є достатньо деталей. Якщо ні, необхідно надати додаткову інформацію до процедури.

Також необхідно переконатись, що кожен, хто може виконати процедуру, має належний доступ / дозволи. [15]

Подібно до політики безпеки слід регулярно переглядати та оновлювати процедури безпеки. Технологічні зміни в організації обумовлюють необхідність оновлення процедур, і нові процедури слід створювати як частину загального плану впровадження нової технології. Підтримання поточних процедур безпеки забезпечить захист організації від ненавмисних дій чи інших помилок, пов’язаних із здійсненням контролю за безпекою, особливо у стресових ситуаціях.

4.5 Висновки до розділу 4

В четвертому розділі розглянуто питання необхідності політик безпеки у компаніях, спеціальні політики безпеки та процедури безпеки. Зазначено, що політика безпеки – це сукупність норм і правил, що визначають прийняті в організації заходи щодо забезпечення безпеки інформації, пов'язаної з діяльністю організації. Кожна компанія налаштовує політики безпеки під забезпечення своїх цілей та потреб, створюючи спеціальні політики безпеки, що конкретно визначають різні аспекти політик безпеки (наприклад, визначається політика віддаленого доступу, шифрування, користування VPN тощо).

Важливою складовою політик безпеки є процедури безпеки. Вони детально, тобто по крокам, описують як впровадити, увімкнути чи застосувати засоби контролю безпеки організації згідно політики безпеки.

ВИСНОВКИ

У першому розділі розглянуті питання мережевої взаємодії, важливість аналізу кіберзагроз та типові загрози кібербезпеці.

Основу мережевої взаємодії складають моделі ISO/OSI та TCP/IP. Вони розділяють питання обміну інформації на рівні, кожен з яких має справу з певним аспектом зв'язку та реалізується певними протоколами.

Аналіз загроз кібербезпеки є одним із головних процесів забезпечення безпеки, адже саме завдяки аналізу можна ввести превентивні заходи та забезпечити захист від можливих загроз, що можуть призвести до збитків. До аналізу загроз входять: збір фактичної інформації про кібератаки та загрози, перевірка інформації та оцінка поточного впливу, аналіз процедур та політик безпеки на відповідність стандартам безпеки, введення превентивних заходів.

Також, під час розглядання загроз кібербезпеці, визначено, що основну небезпеку складають не тільки технічні загрози(шкідливе програмне забезпечення, фішинг, DDoS атаки, SQL-ін'єкції, атаки типу «людина посередині»), а й загрози, викликані людським фактором(незадоволені, халатні чи низькокваліфіковані співробітники).

У розділі 2 розглянуті програмно-апаратні, мережеві та хмарні засоби захисту. Засоби захисту інформації - це лінійка пристроїв і пристосувань, приладів та технічних систем, а також інших виробів, що застосовуються для вирішення різних завдань із захисту інформації.

Програмно-апаратні засоби (брандмауер, служби фільтрування контенту, системи IDS та IPS, Honeypot) фільтрують та, якщо необхідно, блокують вхідний та вихідний несанкціонований трафік, виявляють та запобігають незаконним вторгненням до системи та відволікають зловмисників від реальних систем.

Мережні засоби захисту (технологія VPN, контроль мережевого доступу та безпека бездротової точки доступу) забезпечують захист всіх кінцевих пристроїв, що мають доступ до мережі від присутніх всередині

загроз безпеки, створюють надійні зашифровані канали за допомогою таких технологій як VPN та контролюють безпечні бездротові з’єднання у інфраструктурі компанії.

Також проаналізовані переваги хмарних технологій захисту інформації (SaaS, PaaS, IaaS, Secaas). До них відносяться можливість завжди отримувати високотехнологічне та оновлене до останньої версії ПЗ, легкість налаштування та масштабування, швидкість відновлення після збоїв.

У третьому розділі розглянуто питання навчання робітників організацій навичкам кібербезпеки. Зазначено, що велика кількість цифрових атак на компанію здійснюються за допомогою соціальної інженерії, де у хід йде психологічний вплив та різні засоби маніпулювання. Найчастіше технічні засоби не можуть допомогти уникнути таких загроз. Саме тому необхідне навчання співробітників. Навчання допоможе співробітникам виявити додатки з шкідливим ПЗ, фішинг, спам та не стати жертвами маніпуляцій, дасть змогу вирішити інцидент одразу після його виникнення.

Важливим елементом є створення культури обізнаності у сфері кібербезпеки. Це стимулює робітників завжди покращувати свої навички та бути обізнаними у цій галузі.

В четвертому розділі розглянуте питання необхідності політик безпеки, у компаніях, спеціальні політики безпеки та процедури безпеки. Зазначено, що політика безпеки - це сукупність норм і правил, що визначають прийняті в організації заходи щодо забезпечення безпеки інформації, пов'язаної з діяльністю організації. Кожна компанія налаштовує політики безпеки під забезпечення своїх цілей та потреб, створюючи спеціальні політики безпеки, що конкретно визначають різні аспекти політик безпеки(наприклад, визначається політика віддаленого доступу, шифрування, користування VPN тощо).

Важливою складовою політик безпеки є процедури безпеки. Вони детально описують як впровадити, увімкнути чи застосувати засоби контролю безпеки організації згідно політики безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. ЗАКОН УКРАЇНИ Про телекомунікації // Відомості Верховної Ради України (ВВР), 2004, № 12, ст.155.

2. Natarajan Meghanathan. A Tutorial on Network Security: Attacks and Controls // Jackson State University - 2014.

3. Олифер В., Олифер Н.Компьютерные сети. Принципы, технологии, протоколы: 5 издание

4. ЗАКОН УКРАЇНИ Про основні засади забезпечення кібербезпеки України // Відомості Верховної Ради (ВВР), 2017, № 45, ст.403.

5. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. — М.: ИД «ФОРУМ»: ИНФРА-М, 2011. — 416 с.

6. Aakanksha Chopra - Security Issues of Firewall // International Journal of P2P Network Trends and Technology (IJPTT) – Volume 22 Number 1 January 2016

7. Rathod, R.H., & Deshmukh, Prof. V.M. (2013). Role of Distributed Firewalls in Local Network for Data Security. International Journal of Computer Science and Applications, Vol. 6, No. 2, Apr 2013, ISSN: 0974-011 (open access), pp: 360-364

8. Sharad Gore et al, ― Importance of Intrusion Detection System‖ International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011.

9. R. Joyce, Virtual Private Networks, Computer Science/Software Engineering, University WisconsinPlatteville, 03 November 2007

10. Virtual Private Networking: An Overview, Sept, 2001, Microsoft:http://technet.microsoft.com/enus/library/bb742566.aspx accessed 01/June/2014

11. Jeamy Heary – Cisco NAC Appliance: Enforcing Host Security With Clean Access // Cisco Press CCIE No. 7690

12. Prof. J. Naren Layers of Cloud – IaaS, PaaS and SaaS: A Survey // (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4477-4480

13. Christian Senk Adoption of security as a service k Journal of Internet Services and Applications 2013, 4:11

14. Puhakainen, P. Design Theory for Information Security Awareness, 2006. Ph.D Thesis, the University of Oulu, Finland.

15. E. Al-Shaer,et al ―Network Security Policies-Verification, Optimization and Testing‖, Network Operation and Management Symposium, page 584, 3-7 April 2006