АКТУАЛЬНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ТЕЛЕКОМУНІКАЦІЙНІЙ ГАЛУЗІ

Куля Ю.Е.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна.

E-mail: yuliia.kulia@nure.ua

Abstract

The purpose of this paper is to provide advice on current risks and highlight potential future threats affecting the telecommunications industry, and to explain how ISPs can use Threat Intelligence to help protect their digital environment and critical infrastructure from emerging cyber threats.

Телекомунікаційна галузь підтримує зв'язок світу. Від приватного спілкування до ділової взаємодії, це невід'ємна частина нашого повсякденного життя, і ми сприймаємо багато елементів як належне. Будь то телефон, Інтернет чи ефір, цей сектор дає змогу швидко спілкуватися в будь-якій точці світу.

Від супутникових компаній, інтернет-провайдерів, телефонних корпорацій, інфраструктура, що стоїть за цими організаціями, робить можливим надсилання всіх наших відео, аудіо та тексту по всьому світу. Що сприяє розвитку практично в кожній галузі. За останні роки, у міру розвитку технологій, наш світ виріс, і в міру того, як змінився вид загроз, різко почастішали кібератаки, спрямовані саме на телекомунікаційну галузь. Враховуючи, що ця галузь контролює переважну більшість складної та критичної національної інфраструктури, вплив успішної атаки є не лише значним, але й масштабним. Але захистити телекомунікаційну інфраструктуру далеко не просто. Галузь розуміє, що жодна загроза не може бути подолана ізольовано, і що суб'єкти загроз продовжуватимуть використовувати вразливі місця в прийнятих технологіях для досягнення своїх цілей.

Карта телекомунікаційних загроз і системи кіберризиків зливаються. Необхідна швидкість і можливості зберігання безмежні. Оператори зв'язку перетворюються з мережевих компаній на компанії хмарних послуг, щоб підвищити ефективність бізнес-операцій, розгорнути нові послуги та програми, а також зберігати та розповсюджувати контент. Оскільки телекомунікаційні зв'язки часто є шлюзом до кількох компаній, загрози можуть бути націлені на конкретну телекомунікаційну компанію, її сторонніх постачальників або абонентів телекомунікаційних послуг. Ці напади мають різні форми. Нижче наведено деякі з найпоширеніших векторів атак.

Інтернет речей

Одним із найбільших викликів для телекомунікаційних компаній та постачальників послуг Інтернету у нинішній ситуації є те, як Інтернет речей вплине на галузь. Інтернет речей стрімко зріс з точки зору його застосування з підключеними пристроями, створюючи більше точок входу в процес. Не всі ці точки виправляються належним чином, і вони залишають облікові записи користувачів, клієнтів і компаній відкритими.

«47% найбільш вразливих пристроїв – це камери безпеки, встановлені в домашніх мережах, за ними йдуть розумні хаби (15%), як-от Google Home і Amazon Alexa, і мережеві пристрої зберігання даних (12%)» – звіт GDPR PrivSec [1].

Внутрішні загрози

Проблема в телекомунікаційних компаніях також полягає в тому, що багато співробітників/інсайдерів взагалі не усвідомлюють, що вони є загрозою. Мало хто в галузі проходить навчання щодо заходів кібербезпеки. І оскільки понад 30% людей зараз працюють віддалено, кількість підключень до незахищених мереж є більшою, ніж будь-коли.

Емпіричні докази ризиків незахищеного Wi-Fi викликають занепокоєння – не лише тому, що багато програм не шифрують передані дані, але й тому, що люди продовжують використовувати мережі» [2].

Ризик третіх сторін

Треті сторони, зокрема постачальники, партнери, постачальники електронної пошти, постачальники послуг, веб-хостингу, юридичні фірми, компанії з управління даними та субпідрядники можуть легко стати доступом у важливу інфраструктуру, куди зловмисники можуть проникнути. Підтримувати безпеку вашої компанії та безпеку постачальників, які беруть участь у бізнесі, може бути складно. Ось чому керовані служби безпеки необхідні для моніторингу всіх елементів даної мережі.

DDoS

Поширеними є DDoS, включаючи відмову в обслуговуванні з розширеним розподіленим відображенням (DrDoS) з використанням стандартних мережевих протоколів і мереж ботів, що складаються із скомпрометованих мобільних пристроїв і пристроїв Інтернет речей. Клієнти очікують безперебійної роботи послуг 24/7. Будь-яке переривання або збій, що впливає на якість обслуговування, може призвести до великих фінансових втрат.

Нещодавній приклад включає атаку на операторів зв'язку в Північній Америці, які, як повідомляється, постраждали від кібератаки розподіленої відмови в обслуговуванні, що вважається найбільшою кібератакою на операторів зв'язку Америки на сьогоднішній день. Крім того, за повідомленнями, атака спричинила збої в мережі мобільного зв'язку в таких штатах, як Флорида, Джорджія, Нью-Йорк, Атланта, Чикаго, Маямі, Форт-Лодердейл, Лос-Анджелес, Каліфорнія та Х'юстон, Техас». Повідомляють Cyber Security Insiders.

Тероризм

За допомогою віддаленого проникнення зловмисники можуть контролювати фізичні елементи, які можуть впливати на критичну інфраструктуру та маніпулювати результатами. А також отримати цінну інформацію про інтелектуальну власність, торгові угоди та особисті дані.

Це лише кілька загроз. Існує ще багато вразливостей, на які повинні звернути увагу постачальники телекомунікацій.

Неправильна конфігурація служб

Злом облікових даних або пристроїв абонента за допомогою соціальної інженерії, фішингу, шкідливого програмного забезпечення.

Довгострокові шпигунські кампанії

Деякі з цих атак є безцільними та походять від злочинців низького рівня, але в багатьох випадках постачальники послуг зв'язку часто стають мішенню висококваліфікованих груп загроз. У результаті існує велика ймовірність того, що багато успішних порушень телекомунікаційної інфраструктури взагалі ніколи не будуть виявлені [3].

Висновки

Захист від загроз, зменшення поверхні атаки та системи безпеки великих, складних і багатогранних організацій не є швидким рішенням. Вартість також є фактором, що не сприяє, оскільки багато організацій мають обмежені ресурси та не можуть забезпечити внутрішній захист своїх пристроїв, систем, людей і процесів.

Це те, що надають постачальники керованої безпеки. Завдяки правильному аналізу загроз телекомунікаційні компанії можуть покращити свій бізнес-профіль, приймати бізнес-рішення на основі точних

даних і надати команді безпеки можливість швидко й точно вирішувати кіберзагрози та миттєво їх пом'якшувати.

Література

1. Aosphere. Звіт GDPR PrivSec [Електронний ресурс] / Aosphere. – 2023. – Режим доступу до ресурсу:https://www.aosphere.com/aos/dp?gad_source=1&gclid=CjwKCAjw7oeqBhBwEiwALyHLMyhvCNFZXVcnU7_WpM0gpv6jj7s8zLHW403dDCanYgMVhi6IPRBYhoCt30QAvD_BwE

2. Kovacs E. 70 Percent of IoT Devices Vulnerable to Cyberattacks: HP [Електронний ресурс] / Eduard Kovacs. – 2014. – Режим доступу до ресурсу: https://www.securityweek.com/70-iot-devices-vulnerable-cyberattacks-hp/.

3. Cyber Crime & Security [Електронний ресурс] // Statista. – 2023. – Режим доступу до ресурсу: https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#overview.