УДК 621.39

РЕКОМЕНДАЦІЇ ЩОДО ПОКРАЩЕННЯ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Григоренко О.Г., Полікарпова Ю.Г.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: olenagri@ukr.net, july.polik@gmail.com

Описані основні загрози, пов’язані з телекомунікаційною інфраструктурою. Зазначені рекомендації щодо покращення безпеки телекомунікаційних мереж.

Recommendations for improving the security of telecommunications networks

The main threats related to the telecommunications infrastructure are described. Recommendations for improving the security of telecommunications networks are defined.

Загрози для безпеки телекомунікаційних мереж є підставою для занепокоєння міжнародних організацій протягом останніх десятиліть. Телекомунікаційна інфраструктура, яка забезпечує необхідну основу для обміну інформацією є особливо вразливою для різних форм нападів. Деякі з цих нападів можуть призвести до відмови в обслуговуванні, втрати цілісності та конфіденційності даних та мережевих служб. Одним із контрзаходів є конфіденційність за замовчуванням, метою якої є оновлення системи при щойно виявлених загрозах.

Загрози, пов'язані з телекомунікаційною інфраструктурою, можуть здійснюватися зловмисниками з метою створення повної відмови зв'язку або отримання незаконного прибутку. Серед таких основних загроз можуть бути виділені [1,2,4]:

1. Теракти. Атаки, які здатні викликати серйозні збої мережевих сервісів, можуть бути будь-якої форми. Однією з форм є атаки в результаті військових конфліктів, що призводять до фізичного руйнування телекомунікаційного обладнання і здійснюються з боку терористів.

2. Технологічні загрози. Є наслідком самих технологій і в основному пов’язані зі споживачами телекомунікаційних послуг. У деяких випадках загроза або напад може привести до великих фінансових втрат. Прикладом може слугувати довготривалий виклик, коли «компанія-одноденка» під виглядом телекомунікаційної організації телефонує абонентам, здійснює переадресацію виклику та пропонує свої послуги. Далі така компанія може утримувати виклик без згоди або відома абонента, і такий виклик може залишатися дійсним протягом декількох днів, якщо у абонента не встановлений ліміт на дзвінок. У разі міжнародного виклику це може привести до серйозної фінансової втрати, адже абонентом може бути як окрема людина, так і організація.

3. Кримінальні злочини. Становлять небезпеку для телекомунікаційних підприємств та їх клієнтів. Наприклад: зрощення телекомунікаційного кабелю, тобто сплайсинг, і хакерство.

Зрощення телекомунікаційної кабельної розводки є процесом

отримання несанкціонованого доступу до телекомунікаційної мережі шляхом механічного приєднання до кабелю. Хакери отримують віддалений доступ до мережі, проникають всередину та компрометують і викрадають дані.

Конвенція про кіберзлочинність Ради Європи виділила вісім правопорушень з подальшою кримінальною відповідальністю: 1) незаконне перехоплення; 2) втручання в дані; 3) втручання в систему; 4) неправильне використання пристроїв; 5) підробка з використанням комп'ютерів; 6) шахрайство з використанням комп'ютерів; 7) правопорушення, пов'язані з дитячою порнографією; 8) правопорушення, пов'язані з порушенням авторського права і суміжних прав.

4. Загальні загрози та атаки. Учасниками є спеціальні державні структури. Це форма хактивізму, що спонсорується державою.

Рисунок 1 надає архітектуру безпеки, що показує, на яких рівнях потрібно вживати заходів для безпечного функціонування додатків і обміну, обробкою даних в мережі організації.

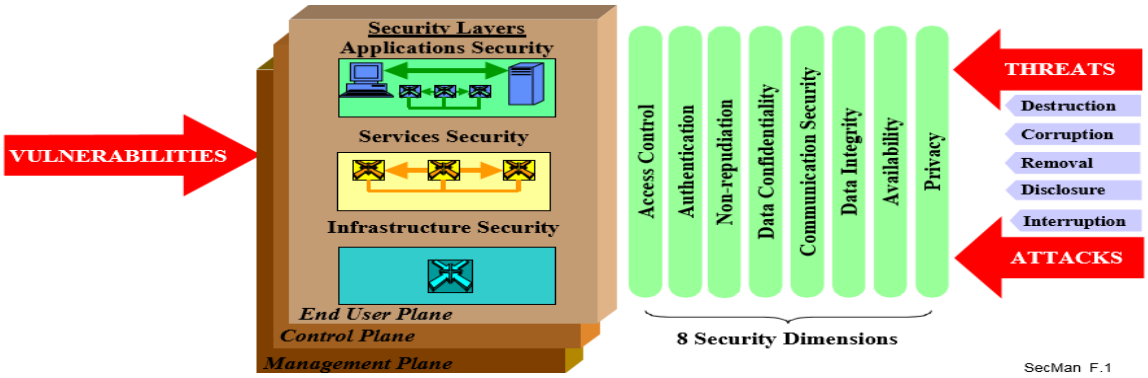

Рис.1. Елементи архітектури безпеки згідно X.805 [3].

Рекомендації щодо покращення безпеки телекомунікаційної мережі полягають в наступному:

1. Телекомунікаційна мережа безпеки.

Необхідна технологія повинна бути введена в дію для збереження телекомунікаційної інфраструктури і ресурсів. У тих регіонах, де є військові конфлікти з високою імовірністю терактів, телекомунікаційна інфраструктура на відкритому повітрі, радіоапаратура і енергогенеруючі комплекти, повинні бути розташовані у більш безпечних районах. Це необхідно, щоб уникнути фізичного знищення встановленого обладнання.

2. Операційна безпека (Operations Security, OPSEC).

OPSEC спрямована на запобігання витоку важливої інформації або процедур, що стосуються безпеки організації із зовнішнім світом. Наприклад, організація може обмежити той контент, який співробітники розміщують на своїх сторінках Facebook або інших соціальних засобах масової інформації.

3. Безпека за замовчуванням.

Організації або компанії повинні розробити систематичний метод профілактики або боротьби з нападом. Безпека за замовчуванням фокусується на трьох пунктах: 1) запобігання: проектування систем, які

важче зламати; 2) стійкість: системи проектування, які можуть запропонувати безпечні транзакції, навіть після того, як вони були скомпрометовані; 3) регенерація: системи проектування, які можуть автоматично відновити себе, коли порушення будуть виявлені.

4. Обмеження на чутливі зони.

Телекомунікаційний простір, обладнання, приміщення повинні бути надійно захищені і розглядатися як обмежені зони. Доступ до цих областей слід контролювати і надавати тільки уповноваженим особам. Такі методи, як установка управління електронного доступу (Electronic Access Controls, EAC), механічні комбінації замків, повинні бути використані для контролю доступу. Список осіб, які мають доступ до цих чутливих зон або приміщень, повинен бути збережений, щоб уникнути несанкціонованого доступу. Організація повинна також вести журнал контролю для цілей аудиту безпеки.

5. Реалізація інфраструктури безпеки [2].

Важливі політики, прийняті організацією, повинні підтримуватися інфраструктурою безпеки мережі, яка включає в себе кілька рівнів безпеки. Ця стратегія говорить про те, що жоден із рівнів безпеки не повинен відкрити мережу для атак. Деякі із заходів безпеки, які можуть бути розгорнуті на різних рівнях: 1) захищена кабельна інфраструктура; 2) фізичні механізми контролю доступу, такі як смарт-картки і біометричні зчитувачі; 3) брандмауери на периметрі мережі для публічно доступних систем; 4) хости і мережеві системи виявлення вторгнень/захисту; 5) управління зловмисними кодами за допомогою антивірусів, антишпигунських технологій; 6) безпечні методи розробки додатків; 7) проведення перевірок безпеки телекомунікаційного обладнання, території, допустимих мережевих компонентів і додатків; 8) шифрування і маскування даних; 9) розуміння безпеки.

Таким чином, телекомунікаційні мережі є великою мішенню для кіберзлочинців, тому усвідомлення сучасних загроз та створення системи заходів безпеки допоможуть організаціям зберегти конфіденційність своїх даних та забезпечити безпечне функціонування мережевої інфраструктури. Запропоновані заходи значно покращать безпеку телекомунікаційної мережі.

Література

1. Григоренко О.Г., Пчелінцев І.С. Заходи для захисту від атак для забезпечення кібербезпеки організацій// МНТК "Перспективи телекомунікацій-2019" - Київ; Дата проведення: 17.04.2019.
2. Security in Telecommunications and Information Technology/ [Електронний ресурс] – Режим доступу: https://www.itu.int/itudoc/itu-t/85097.pdf.
3. ITU-T. X.805 Security architecture for systems providing end-to-end communications.
4. Северина С.В. Інформаційна безпека та методи захисту інформації /С.В.Северина// Вісник Запорізького національного університету. - 2016. - № 1 (29). – С.155-161. [Електронний ресурс] – Режим доступу: http:// www.irbis-nbuv.gov.ua › cgi-bin › irbis_nbuv › cgiirbis_64 › Vznu_.