МЕТОДИ ЗМЕНШЕННЯ РИЗИКІВ БЕЗПЕКИ ДАНИХ ДЛЯ ТЕЛЕКОМУНІКАЦІЙНИХ КОМПАНІЙ

Куля Ю.Е.

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

E-mail: yuliia.kulia@nure.ua

Abstract

The urgency of protecting the telecommunications industry from cyberattacks is one of the most important tasks, due to the fact that this industry works with a large amount of confidential information. With millions of customers sharing personal and financial data with them, telecommunications companies are constantly being targeted by cybercriminals.

Існуючі небезпеки

Телекомунікаційна галузь є одним із найбільших збирачів конфіденційної інформації у світі. Оскільки мільйони клієнтів діляться з ними особистою інформацією та фінансовими даними, телекомунікаційні компанії постійно стають мішенню кіберзлочинців.

За даними фірми з кібербезпеки EfficientIP, у 2023 році 43% операторів зв'язку постраждали від атак зловмисного програмного забезпечення на основі системи доменних імен (DNS), причому приголомшливим 81% знадобилося три дні або більше, щоб застосувати критичний захід безпеки після виявлення порушення даних. Той самий звіт показав, що в телекомунікаційному секторі крадуть найбільше конфіденційних даних у всіх галузях: 30% телекомунікаційних компаній, які брали участь в опитуванні, повідомили про крадіжку конфіденційної інформації про клієнтів.

Звіт Windows Defender [1] також показав, що кіберзлочинці часто вербують інсайдерів для атаки на телекомунікаційних провайдерів. Хакери перетворюють незадоволених співробітників на зловмисних інсайдерів або шантажують персонал, використовуючи компрометуючу інформацію, зібрану з відкритих джерел. Майже 28% усіх кібератак, націлених на телекомунікації, стосувалися зловмисної діяльності інсайдерів на момент публікації звіту.

Але такі атаки – не єдине, про що слід хвилюватися телекомунікаційним компаніям. Конфіденційні дані, такі як ідентифікаційна та фінансова інформація, також захищені відповідно до законів про захист даних і міжнародних стандартів. Від Загального регламенту захисту даних ЄС (GDPR) до бразильського Lei Geral de Proteção de Dados (LGPD) і японського Закону про захист персональних даних (APPI) захист персональних даних став юридичним зобов'язанням у всьому світі. Недотримання цих законів може призвести до великих фінансових санкцій і шкоди репутації.

Що стосується фінансової інформації, стандарт безпеки даних індустрії платіжних карток (PCI DSS) був створений найбільшими світовими брендами карток для забезпечення захисту платіжних систем від злому, шахрайства та крадіжки даних власників карток. Незважаючи на те, що PCI DSS не є юридично зобов'язуючим, він є загальним стандартом, прийнятим постачальниками фінансових послуг у всьому світі, і його дотримання є обов'язковим для будь-якої організації, яка бажає приймати платежі кредитною чи дебетовою карткою особисто, по телефону чи онлайн.

З усіх цих причин безпека даних повинна бути першочерговою турботою для сектору телекомунікацій. Але як телекомунікаційні компанії можуть мінімізувати ці кіберризики та уникнути втрати даних? Ось наші рекомендації.

Обмеження передачі конфіденційних даних

Людський фактор часто є найслабшою ланкою в стратегії кібербезпеки. Телекомунікаційні компанії можуть обмежити шкоду, яку можуть заподіяти співробітники, запровадивши рішення із запобігання втраті даних – Data Loss Prevention (DLP).

Технологія DLP безпосередньо захищає конфіденційні дані. Телекомунікаційні компанії можуть вибирати попередньо визначені профілі для конфіденційної інформації, такої як ідентифікаційна інформація та дані кредитних карток, а також профілі, орієнтовані на дотримання законів про захист персональних даних. Потім переміщення файлів, що містять конфіденційну інформацію, можна відстежувати в режимі реального часу, а їх передачу можна обмежити або заблокувати. Таким чином, телекомунікаційні компанії можуть заборонити співробітникам ділитися конфіденційною інформацією через програми обміну повідомленнями, служби обміну файлами, особисту електронну пошту тощо [2].

Управління знімними пристроями

Ще один спосіб, за допомогою якого співробітники можуть викрадати дані, — це знімні пристрої. USB-накопичувачі, зокрема, легко сховати та загубити, що робить їх ідеальним інструментом для крадіжки даних і постійним джерелом втрати даних. Щоб запобігти співробітникам використання USB або обмежити використання надійних пристроїв компанії, телекомунікаційні компанії можуть скористатися рішеннями DLP.

Інструменти DLP оснащені функціями керування пристроями, які дозволяють компаніям блокувати або обмежувати використання портів USB і периферійних пристроїв, а також з'єднань Bluetooth. Не дозволяючи співробітникам підключати персональні знімні пристрої, які не відповідають стандартам безпеки компанії та можуть бути джерелом зараження мережі, телекомунікаційні компанії можуть допомогти захистити дані.

Кросплатформні можливості

Телекомунікаційні компанії часто працюють у середовищі змішаних операційних систем. Більшість продуктів безпеки зосереджені на конкретній операційній системі – часто Windows, яка є основною операційною системою на підприємстві – і пропонують лише скорочені версії для інших операційних систем.

Це може наражати комп'ютери, що працюють на інших операційних системах, на витоки даних. Хоча деякі операційні системи менш вразливі до зовнішніх загроз безпеки, дані, що зберігаються в них, так само піддаються недбалості з боку інсайдерів, а також кібератакам, націленим на співробітників, наприклад тим, що базуються на фішингу та соціальної інженерії [3].

Висновки

Підводячи підсумки можна сказати, що телекомунікаційним компаніям важливо обирати послуги безпеки даних, щоб забезпечити однаковий рівень захисту для всіх операційних систем у їхній мережі. Це може перетворитися на кілька продуктів, кожен з яких спеціалізується на одній ОС або крос-платформних рішеннях.

Література

1. Працездатності пристрою, звіт про працездатність антивірусної програми у Microsoft Defender. Режим доступу: *https://learn.microsoft.com/ru-ru/defender-endpoint/device-health-microsoft-defender-antivirus-health*

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

3. Aosphere. Звіт GDPR PrivSec [Електронний ресурс] / Aosphere. – 2023. – Режим доступу до ресурсу:https://www.aosphere.com/aos/dp?gad_source=1&gclid=CjwKCAjw7oeqBhBwEiwALyH MyhvCNFZXVcnU7_WpM0gpv6jj7s8zLHW403dDCanYgMVhi6IPRBYhoCt30QAvD_BwE