ВИЯВЛЕННЯ АНОМАЛІЙ ТРАФІКУ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

магістр Р.О. Ковтун, канд. фіз.-мат. наук, доц. О.П. Черних,
Національний технічний університет "Харківський політехнічний інститут", м. Харків

В даний час одним із актуальних напрямів в області забезпечення інформаційної безпеки є виявлення атак і запобігання вторгнень зловмисника в комп'ютерні системи і корпоративні мережі.

Для виявлення відомих і невідомих атак використовують ряд спеціалізованих алгоритмів і засобів: поведінкові та сигнатурні методи, методи виявлення аномальної активності, які особливо ефективні для виявлення інсайдерських атак і атак "нульового дня".

Аномалія – відступ або відхилення від правила, тому аномальним називають все відступаюче від правильного або нормального.

За своєю суттю аналіз аномалій дозволяє виявляти значні відхилення трафіку мережевих пристроїв від "нормального" профілю трафіку для пристрою або групи пристроїв.

Як правило, шаблон "нормального" трафіку мережі складається протягом певного проміжку часу на основі статистичних даних та навчальної вибірки.

Для виявлення аномалій в більшості випадків досить аналізувати основні параметри трафіку (телеметрію) і немає необхідності вивчати вміст кожного пакета.

Прикладами аномалій, виявлених на основі аналізу телеметрії трафіку, є раптове збільшення інтенсивності трафіку від робочої станції або зміна структури трафіку в порівнянні зі звичайними щоденними показниками для даної мережі або пристрою. При виявленні мережевої аномалії, з метою прийняття рішення про подальші дії необхідно ретельно вивчити її природу, потенційну небезпеку та можливі наслідки.

В якості основних класифікаційних ознак використовують тип джерела, причина виникнення, область (місце) виникнення, спосіб прояви, характер змін.

Дана інформація дає можливість системному інженеру швидко та своєчасно реагувати на аномалії трафіку, виявляти потенційні мережеві атаки та вживати необхідні заходи щодо їх усунення.