МЕТОДИ ВИЯВЛЕННЯ ВТОРГНЕНЬ У ХМАРНИХ СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

К. О. Маковоз
м. Кривий Ріг, Криворізький національний університет
girl_karina@mail.ru

Системи відеоспостереження – це комплекс обладнання та програм, яке використовують для організації охоронного відеоспостереження на об'єктах, незалежно від їхнього територіального розташування.

Хмарна інфраструктура може бути ефективно використана для масштабування системи відеоспостереження в наступних вимірах:

– зберігання відео і метаданих відеоаналітики;

– підключення нових об'єктів спостереження (наприклад, торгових точок);

– реалізація нових функцій аналізу метаданих і пошуку в архіві;

–обслуговування великого числа користувачів.

Проте навіть такий спосіб охорони, як відеоспостереження, може виявитись небезпечним. Досвідченим хакерам вистачить не так багато часу, щоб заволодіти «конфіденційною» інформацією з камер відеоспостереження та серверів, де зберігаються відеофайли. Прикладами зломів та атак на цифрові канали передачі даних є, наприклад, підміна зображення в мережі відеоспостереження, перехвату телеконференцій (перехоплюючи зображення учасників, що спілкуються в реальному часі). Великими втратами може скінчитись для організації злом відеосерверів.

Одна з причин взломів та атак в тому, що в більшості систем безпеки застосовують стандартні механізми захисту. Звідси потреба в механізмах, які, доповнюючи традиційні, робили б можливим виявлення спроб несанкціонованого доступу та інформували про це відповідальних за безпеку. Важливо, щоб такі системи могли протистояти атакам, навіть якщо зловмисник вже був аутентифікований, авторизований і з формальної точки зору дотримання прав доступу мав необхідні повноваження на свої дії. Ці функції виконують системи виявлення вторгнень – це системи, що збирають інформацію з різних точок захищеної комп'ютерної системи (мережі) і аналізують цю інформацію для виявлення як спроб порушення, так і реальних порушень захисту (вторгнень).

У сучасних системах виявлення виділяють наступні основні елементи: підсистема збору інформації для збору первинної інформації про роботу захищеної системи; підсистема аналізу (виявлення) здійснює пошук атак і вторгнень в захищену систему; підсистема подання даних, дозволяє користувачам стежити за станом захищеної системи.