УДК 004.056.53

Юрій Валерійович ГНУСОВ,
кандидат технічних наук, доцент,
завідувач кафедри інформаційних технологій та кібербезпеки
факультету № 4 Харківського національного університету внутрішніх справ

Сергій Володимирович КАЛЯКІН,
викладач кафедри інформаційних технологій та кібербезпеки
факультету № 4 Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ КІБЕРАТАК НА МІСЬКУ ІТ-ІНФРАСТРУКТУРУ

Автоматизовані системи управління досить широко використовуються для регулювання різних процесів в сучасному місті. Все більше он лайн сервісів впроваджуються в міську ІТ-інфраструктуру. Це стало причиною того, що останнім часом кіберзлочинні угруповання та хакери-одинаки все частіше обирають їх ціллю своїх атак.

В 2019 році близько 20 муніципалітетів в США зіткнулося з проблемою шифрувальників. Найбільш гучна атака сталася 7 травня у місті Балтімор, де спрацював кріптолокер «Робін Гуд» (RobbinHood). У той же день муніципалітет Балтімора повідомив ФБР і відключив частину своїх систем, вважаючи, що таким чином зможе зупинити поширення шкідливого програмного забезпечення, яке наразі вже встигло заразити голосову та електронну пошту, систему оплати штрафів, систему оплати рахунків за воду, систему відеоспостереження, а також систему оплати податків за нерухомість, через що більше 1500 угод з нерухомістю було зупинено. Зловмисники вимагали викупу в розмірі трьох біткоїнів за кожну з атакованих систем або 13 біткоїнів за повернення доступу до всіх систем відразу.

Шифрувальник почав своє поширення через фішингову атаку, спрямовану на одного зі службовців муніципалітету. Чи була віна цілеспрямованою або випадковою - невідомо. При цьому, частина ІТ-інфраструктури була розміщена в хмаровому сервісі Amazon, але муніципалітет і її майже

втратив, тому що на початку травня завершився контракт на підтримку, який не змогли продовжити через непрацюючі систем оплати рахунків.

Причиною усіх цих неприємностей, як вважають спеціалісти з ІБ, стали декілька чинників.

По-перше, за останні 7 років 4 CIO (Chief Information Officer) Балтімора були звільнені або пішли самостійно, двоє досі знаходяться під слідством (за неправомірні витрати і сексуальні домагання). Таким чином, нормально розвивати ІТ та ІБ в Балтіморі не вдавалося - майже кожні 1,5 року начальство, яке визначає шлях розвитку ІТ-інфраструктури міста, змінювалося. Ще у 2017-му році компанія Gartner розробила для Балтімора 5-річний план розвитку, але реалізувати його так і не вдалося.

По-друге, в бюджеті міста лише 2,5% виділялося на ІТ (включаючи витрати і на ІБ), що вдвічі нижче середніх цифр американських міських бюджетів. Менеджер по ІБ на бюджетному комітеті просив грошей на заходи по ІБ, але йому було відмовлено.

По-третє, пропозиції щодо підвищенні обізнаності муніципальних службовців теж не отримали підтримки через брак коштів.

На засіданні міського бюджетного комітету 29 травня чиновники Балтімора підрахували, що напад може коштувати місту 18,2 мільйона доларів. Близько 4,7 мільйона доларів на той момент було вже витрачено.

До речі, в 2018-му році в Балтіморі від шифрувальника вже постраждала одна з систем (служба 911). Сталося це через відключені в процесі підтримки внутрішніх систем правил на MCE (Machine Check Exception). Однак ніяких висновків зроблено не було.

Випадок в Балтиморі не є поодиноким. RobbinHood до Балтімора атакував ще одне американське місто - Гринвиль в Північній Каліфорнії. Плану реагування на інциденти в муніципалітеті не було, що досить дивно. План ручного відновлення був розроблений через два тижні після початку епідемії. Частково виправдати це можна тим, що мер міста вступив на посаду за кілька днів до епідемії RobbinHood (колишній мер пішов у відставку через звинувачення в зростаючій корупції) і багато посад в адміністрації були порожні, що і призвело до такого хаотичного стану.

Лейк-Сіті, штат Флорида, декілька днів відновлювався після атаки іншого шифрувальника TripleThreat 10 червня, який вразив його електронну пошту та онлайн-платіжні системи.

Хмарна компанія з кібербезпеки AppRiver повідомила про TripleThreat минулого січня, але на той момент вважалося, що це фішинг-схема, призначена для збору облікових даних, і про шифрувальний компонент було не відомо.

12 червня місто оновило свій статус, в якому сказано, що, хоча більшість систем все ще не працює, досягнуто прогресу у відновленні мережі та доступу до заблокованих даних. Системи, що обслуговують міську поліцію, пожежну та інші екстрені служби, не постраждали. Відправку електронні листів відновили протягом наступного дня. Намагання з відновлення даних теж були успішними, хоча потрібен певний час, щоб повернути їх у первісний формат.

Таким чином, ми бачимо, що атаки на міську ІТ-інфраструктуру будуть поширюватися і треба бути заздалегідь готовими до них. Забезпечення ІБ міста справа не з дешевих, але витрати на відновлення втрачених даних можуть набагато перевищити витрати на інформаційну безпеку.

Одержано 29.04.2020