електронна пошта та всі контакти, збереженні колись зображення, інформація з календарів і так далі…

Ваші смартфони та ПК несуть за собою ще одну небезпеку. Влада може у будь-який час прослуховувати ваші дзвінки та переглядати файли на вашому смартфоні. Більше того, будь-який навіть не надто навчений хакер може підключитися до камери чи мікрофону на вашому пристрої. Він має змогу робити фотографії без вашого відома, переймати звук з мікрофона та використовувати у своїх цілях. Загалом це відбувається для того, щоб дізнатися якісь паролі чи цікаву інформацію з вашого приватного життя.

Отже, все здіяне вами у мережі приховати не вийде. Кожен крок та кожне навіть випадково відкрите зображення залишить свої сліди глибоко у системі. Можна лише спробувати бути обачнішим. Ніколи не пізно заклеїти веб - камеру та мікрофон, перевіряти на що саме просять дозвіл скачані вами програми. Але від постійного шпигування сховатися все ж не можна. Технології вже надто тісно переплелися з нашим життям.

Тому хотілося б закінчити словами веб - розробника Ділана Каррана:

«Це одна із найбільш божевільних речей сучасної епохи. Ми ніколи не дозволили б уряду або корпорації встановити камери/мікрофони в нашому будинку або відстежувати наше місце розташування. Але ми зробили це за власним бажанням, бо, хай йому грець! – «Я хочу дивитися милі відео з песиками»

Плескачова В.С. – курсант факультету підготовки фахівців для органів досудового розслідування, науковий керівник **Прокопов С.О. -** старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

КІБЕРБЕЗПЕКА «РОЗУМНОГО» МІСТА

Актуальність даної теми зумовлена тим, що в останні десять років у багатьох країнах почали реалізацію проекти з розвитку сучасної міської інфраструктури на базі широкого використання сучасних технологій, особливо засобів інформаційно-комунікаційних технологій (ІКТ). Цей задум, який отримав назву «розумне» місто (Smart City), згуртовує навколо себе міську владу, громадських діячів та бізнесменів. Концепцію Smart City можна визначити як використання цифрових і комунікаційних технологій з метою покращення якості та ефективності міських послуг, зменшення витрат і споживання ресурсів, розширення співробітництва з громадянами. Багато організацій в світі працюють над цими технологіями.

«Розумні» міста визначаються також як «місто знань», «цифрове місто», «кібермісто», «екомісто» – в залежності від цілей міського планування. Вони проводять постійний моніторинг важливих об'єктів інфраструктури – автомобільних доріг, мостів, тунелів, залізниць, метро, аеропортів, морських портів, систем зв'язку, водопостачання, енергопостачання, найважливіших будівель з метою оптимального розподілу ресурсів і забезпечення безпеки. Вони постійно нарощують число надаваних населенню послуг, забезпечуючи стійке середовище, яке сприяє благоустрою і збереженню здоров'я громадян. «Розумними» можуть бути як нові міста, які відразу будуються як «розумні», або, що частіше, звичайні міста, які крок за кроком стають «розумними». Подібні проекти відносяться до інфраструктурних і їхній бюджет становить десятки мільярдів доларів, як при будівництві нових «розумних» міст з нуля, так і при модернізації існуючих міських систем. Реалізуються вони завжди з ініціативи урядів або місцевої влади із залученням бізнес-партнерів.

Зчитування знаків авто в ДТП, розпізнавання обличчя, наближення та наведення різкості – все це вміють камери, які є важливою складовою «розумного» міста. Прикладом є система «Гарпун», яка нещодавно почала використовуватись Національною поліцією України. Для працівників правоохоронних органів це відіграє важливу роль у розкритті злочинів, бо практично вже по всьому місту встановлені відеокамери, до яких має доступ ще й правоохоронець. Ці записи з камер працівник правоохоронних органів може в подальшому використати як доказ при розкритті адміністративного правопорушення чи злочину.

З огляду на сучасні темпи інновацій вже найближчим часом моделі «розумних» міст стануть поширеними реальними і популярними стратегіями міського розвитку. Для того щоб формування «розумних» міст стало наступним етапом процесу урбанізації потрібні і нові стандарти. З огляду на велике значення стандартизації для створення «розумних» міст, різноманітні заходи здійснюються Міжнародною організацією по стандартизації та Міжнародним союзом електрозв'язку.

Проблеми безпеки смарт-міст мають за своєю природою міжнародний рівень і притаманні містам по всьому світу. Громадська інфраструктура, як і раніше, являє собою особливо привабливу мішень для злочинців і терористів. У міру того, як світ стає все більш урбанізованим, міські високотехнологічні центри із цифровими технологіями збільшують вразливість суспільства. Міста є критично важливими інфраструктурами у всіх можливих сенсах, і якщо їх комп'ютеризація проводиться без урахування кібербезпеки з самого початку, проблеми, що можуть виникнути, сягнуть куди більш драматичного розмаху ніж знайомі і часто обговорювані питання кібербезпеки сьогоднішньої критичної інфраструктури. Це завдання треба вирішувати на ранній стадії, інакше вартість і складність створення «розумного» міста може надзвичайно ускладнити вирішення проблем безпеки на наступних етапах реалізації. З Інтернетом речей (IoT), який продовжує стимулювати розвиток розумних міст, міські інфраструктури стають все більш комплексними, але

залишаються легкими для проникнення.

Значна кількість пристроїв Інтернету речей надає можливості атаки на дані мережі. У масштабах міста, в якому тисячі пристроїв спілкуються одночасно як з користувачами, так і між собою, наслідки для безпеки стають значними. Мережа може бути порушена певними хакерами, зловмисниками або й одиночними гравцями. Вразлива кібератака може бути здійснена з одного смартфона або робочого місця. Кожна з функціональних систем розумного міста може викликати інтерес з боку внутрішніх і зовнішніх зловмисників. Вони можуть поставити під загрозу надання послуг, спровокувати серйозні інциденти в наданні критично важливих послуг, створити мережі типу ботнет, які складаються із скомпрометованих пристроїв, і використовувати їх для виконання завдань, відмінних від тих, для яких вони були спочатку призначені [4].

Основними проблемами інформаційних систем «розумних» міст з точки зору кібербезпеки є велика кількість технологій і практичних рішень, які повинні взаємодіяти і зв'язуватися один з одним, нерівна якість різних вбудованих технологій, дистанційна і безпосередня експлуатація інформаційних систем Smart City, величезні обсяги даних для аналізу і зберігання. І всі ці проблеми поряд з багатьма іншими слід розглядати завчасно, до «порозумнішання» кожного міста. Модернізація і «доповнена кібербезпека» не варіант для концепції «розумних» міст. Ризики занадто великі і українські міста повинні використовувати шанс розглядати кібербезпеку з самої ранньої стадії на всіх можливих рівнях.

З метою забезпечення кіберстійкості «розумних» міст з'явилася міжнародна ініціатива Securing Smart Cities, активно підтримувана рядом організацій в усьому світі. Заявленою місією ініціативи є визначення викликів кібербезпеки, що стоять перед «розумними» містами, і вироблення ефективних рішень протидії. Це включає просування кращих практик в галузі кібербезпеки і кіберрішень для всіх технологій, що використовуються в «розумних» містах. Ініціатива націлена на вирішення кіберпроблем на кожному етапі розвитку Smart City – від планування до фактичної реалізації інтелектуальних міст. У кінці листопада 2015 року ініціатори Securing Smart Cities випустили розроблені спільно з Cloud Security Alliance керівні принципи для прийняття за основу технологій «розумного» міста [2].

Використані джерела

1. Концепція Київ Смарт Сіті 2020. – Режим доступу : http://kscf.in.ua/Smart_City_UKR_Print_final.pdf

2. Cyber Security Guidelines for Smart City Technology Adoption. − Access mode : http://securingsmartcities.org/wp-content/uploads/2015/11/

3. Les données numériques : le cœur des villes intelligentes et leur plus grande menace. − Mode d'accès :http://www.lebigdata.fr/les-donnees-numeriques-lecoeur-des-villes-intelligentes-et-leur-plus-grande-menace1911

4.Sécuriser les smart cities. − Mode d'accès : http://www.lesechos.fr/ideesdebats/cercle/cercle-145555-la-securite-des-smart-cities-nouvel-enjeu-pour-lesgouvernements-1183369.php