ЦИФРОВА БЕЗПЕКА У СВІТІ ТА В УКРАЇНІ

Любимов О. С., ст. (гр. КВ-83мп, ФПМ КПІ ім. Ігоря Сікорського)

Інформаційна безпека – дуже важлива в сучасності. Важко уявити навіть одну сучасну людину, яка не користується телефоном, комп'ютером або будь-яким іншим пристроєм що має вільний доступ в мережу Інтернет. Навіть віддалені кутки Землі вже мають, хоч і повільний, доступ в мережу. Тільки в одній соціальній мережі Facebook, за даними на 2018 рік, зареєстровано близько 2.3 мільярдів користувачів.

Та це лише один з світових гігантів-сервісів, що надають соціальні он-лайн можливості. Кількість користувачів у подібних мережах щороку тільки зростає, а з ними зростає і кількість конфіденціальних даних, що оброблюються та зберігаються на серверах онлайн сервісу.

Для кожного втрата конфіденційності може бути різноманітною. Для одного це лише неприємна згадка, для іншого це втрата дуже важливого акаунту, для третього це може бути навіть непід'ємний та досить неочікуваний кредит. Не варто і казати, що персональні данні бувають різними, десь це лише дата народження, десь це контактна база, а на деяких сайтах навіть і платіжна інформація. Та для зловмисників не має нічого не етичного, знайти вигоду можна де завгодно. На закритих сайтах можна знайти акаунти від різноманітних он-лайн сервісі, які продаються тисячами, та зовсім за безцінок.

Нажаль навіть надійний пароль може не захистити від крадіжки даних. Так, наприклад лише за 2018 рік у Facebook сталася один з найбільших витоків даних – а саме данні 50 мільйонів учасників мережі було вкрадено за декілька годин. Нажаль такі ситуації трапляються через невдалий захист, або проблеми у системах валідації користувачів. Хоч компанії і несуть збитки за кожен витік або крадіжку даних, та запобігти таких ситуацій повністю майже неможливо, не тільки тому що це дорого, але й тому що це досить важка та складна задача [1].

Кібернапади та порушення даних стають настільки поширеними, що в будь-який момент може постраждати будь-яка організації. Деякі організації можуть використовувати таку можливість, для того щоб не вкладати кошти в кібербезпеку, але зменшення ризику подальшого нападу це можливо- і цей варіант набагато більш доступний, ніж чекати, поки не буде занадто пізно.

Наприклад, Maersk оголосив, що після атаки вірусуNotPetyaвін втратив до 300 мільйонів доларів,і навіть на сьогоднішній день вони підраховують збитки та усувають наслідки нападу. Дослідження збитків після кібер-нападу у Ponemon Institute у 2017 році показала, що лише британські організації втрачають в середньому 2,48 мільйони фунтів стерлінгів після атаки на данні [2].

Багато організацій що вже прискорено інвестують кошти в кібербезпеку прогнозують, що витрати на кібербезпеку зростуть до 90 млрд. Доларів США в 2018 році. Але нажаль це замало лише бездумно інвестувати гроші у

кібербезпеку, іноді навіть «найкращі» системи світу не можуть дати відсіч анонімному злодію.

Згідно з іншим звітом від Gartner, в середньому організації витрачають 5,6% загального бюджету IT на безпеку та управління ризиками. Це, безумовно, адекватно, але проблема полягає в тому, що 68 мільярдів фунтів стерлінгів, витрачених організаціями на кібербезпеку, набагато менше ніж вартість викрадених або втрачених даних.

В тому ж році було 3,1 мільярда пошкоджених або втрачених, а показники Ponemon виявили, що кожен викрадений запис коштує в середньому 158 дол. США, за нескладними підрахунками слідкує, що компаніями лише за цей рік було втрачено 490 млрд. Доларів. Частка цих грошей було витрачено на усунення наслідків, та інша частка - на штрафи, субсидії та інші види витрат на судові справи.

На сьогодні більшості великих компаній стає дуже складно розвивати імунітет до кібер-атак. Через велику інфраструктуру апаратної та програмної частини – буде легше відбудувати все з початку, а ніж переробляти все що. Та такому методу може стати на заваді висока ціна та великий проміжок часу на розробку.

До покращення кібер-безпеки можна віднести такі методики та новітні технології: розподілені системи, використання провідних технологій шифрування, використання технології блокчейн.

Розподілені системи – повна відмова від централізованих серверів, та перехід на велику кількість маленьких. Кожний, з великої кількості, серверів буде знати стан своїх сусідів, що допоможе запобігти втрачанню одразу усіх даних та своєчасно знайти та вивести з роботи той сервер, що став ціллю нападу. Також через велику кількість та великі відстані між серверами, втручання злодіїв безпосередньо до апаратної частини серверу стає майже не можливим, а методи дублювання даних між випадковими серверами дасть можливість запобігти можливої втрати даних;

Використання провідних технологій шифрування, таких як кінцеве шифрування, яке назараз я досить розповсюдженим у мультиплатформних месенджерах (Telegram, WhatsUp та інші). Кінцеве шифрування означає, що можливість розшифрувати повідомлення є тільки у того, хто являється отримувачем, так ключ до розшифровки більше ніде не знаходиться та не передається через мережу Інтернет;

Використання технології блокчейн. Технологія Blockchain (блокчейн, тобто ланцюг блоків) представляє собою розподілену базу даних, яку можна охарактеризувати як журнал (або навіть бухгалтерську книгу), де кожний запис є унікальним за рахунок часової мітки та хеш коду операції. Записи в цьому «журналі» – це блоки, де кожен не просто унікальний, але і зберігає у собі посилання (ідентифікатор) на попередній блок.

Така методика дозволяє гарантувати незмінність даних, та повний контроль над ними, що широко використовується у новітніх криптовалютах, та заміняє бухгалтерську книгу. Подібна перевага обумовлена наступними

особливостями блоків: кожен блок не тільки тримає у собі посилання на попередній, та й ідентифікатор попереднього блоку, який може бути отриманий завдяки унікальному хеш коду транзакції, який розраховується під час збірки блоку. Тобто підміна блоку означає зміну його хеш ідентифікатора; через це ланцюг блоків розривається за посиланням на неіснуючий блок. Під час завершення обрахунків наступного блоку за одним з двох спеціальних правил відбувається масове розсилання обрахованого блоку між усіма комп'ютерами в мережі, які приймуть його як новий правильний блок і продовжать генерацію та обрахунок нових блоків.

Повертаючись до України, не варто і казати про ступінь її кібербезпеки у порівнянні з зазначеними вище організаціями та країнами, нажаль ще декілька років тому не один з розповсюджених українських ресурсів не можливо було назвати захищеним. Авжеж державні сервіси та закриті проекти були досить захищеними, та такий «захист» справжньому злодію не стане на заваді.

В лютому минулого року було розпочато активну боротьбу з кібер-атаками. Зокрема, Палата представників Конгресу США підтримала законопроект «Ukraine Cybersecurity Cooperation Actof 2017». Цей документ посилює співробітництво між Україною та США і передбачає три ключові напрями:

– вдосконалення систем безпеки урядових систем, в першу чергу тих, які захищають критичну інфраструктуру України;

– зменшення залежності від російських інформаційно-комунікаційних технологій;

– нарощування потенціалу, розширення обміну інформацією щодо кібербезпеки та співробітництво в кіберпросторі.

У випадку ухвалення документа сумарний бюджет його проектів може скласти близько 500 мільйонів доларів протягом 2018–2022 років.

Кілька років тому фахівці у сфері безпеки та оборони з корпорації «РЕНД» працювали в Україні та надали певні рекомендації щодо розвитку напряму кібербезпеки. Частина цих ідей відображена в практичних проектах, які зафіксовані в «Стратегічному оборонному бюлетені України» або «Стратегії кібербезпеки України». Одночасно триває практична реалізація домовленостей, досягнутих за результатами перших українсько-американських міжвідомчих консультацій високого рівня з кібербезпеки, які відбулися 29 вересня 2017 року.

Започатковано дуже своєчасний проект з боку Державного департаменту США(через його відповідний підрозділ з координації питань кібербезпеки) у сприянні з реалізації нашої національної стратегії кібербезпеки на загальнодержавному рівні. Підрядником проекту виступили фахівці відомої американської компанії MITRE, яка надає комплексні консалтингові послуги у сфері безпеки.

Довідково: Команда MITRE провела концептуальну та технічну експертизи з оцінки поточної позиції у кіберпросторі на тлі стратегічного контексту України, нормативно-правової бази, а також у визначенні подальших пріоритетних заходів. За результатами їхнього першого візиту у грудні

минулого року Україна отримала непогану «оцінку». Як зазначено у відповідному звіті, незважаючи на численні економічні та управлінські проблеми, Україна визначила реалістичні стратегічні цілі щодо кіберпростору та має технічний талант для їхнього досягнення, за умови що ці переваги будуть максимально використані для досягнення змін через цілеспрямовані, дисципліновані та спільні зусилля.

Як можна помітити з 2017 року та по сьогодні йде боротьба з кіберзлочинністю на теренах України. До основних пунктів якої можна віднести:

– дезінформація населення через ЗМІ;
– видалення даних;
– крадіжка стратегічно важливих даних;
– втручання у хід державного управління.

Та стоїть пам’ятати, що ціллю кіберзлочину може стати будь-хто і будь-коли, і втрата контактної бази, або банківського акаунти, це ще не так страшно як втрата конфіденційної інформації за якою слідкую крадіжка, вбивство тощо. Не дивлячись на досить не розповсюджену методику, в Україні таке також трапляється. Для запобігання цього звичайний користувач може скористатися такими заходами:

– зміна паролю в акаунтах не більш складний (не менше 8 символів, спеціального знаку та зміна регістру);
– використання двох-факторної авторизації, з допомогою телефону;
– перевірити активність на акаунтах на можливість аномалій, та у разі потреби звернутись у службу підтримки користувача відповідного сервісу.

Такі прості не перший погляд заходи дуже сильно зменшують можливість втручання кібер-злодіїв у кібер-життя звичайної людини.

Науковий керівник: Землянська О. В., ст. викл. (каф. ОППЦБ КПІ ім. Ігоря Сікорського)

Література

1. Facebook HACKED: 50 MILLION account scomprised in majord at abreach! [Електронний ресурс] – Режимдоступу до ресурсу: https://www.express.co.uk/life-style/science-technology/1024277/Facebook-hack-50-million-accounts-targeted-attack-data-breach.
2. How much should organisations spend on cyber security? [Електронний ресурс] – Режим доступу до ресурсу: https://www.itgovernance.co.uk/blog/how-much-should-organisations-spend-on-cyber-security/.
3. Кибербезопасность2017-2018. [Електронний ресурс] – Режим доступу до ресурсу: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-2017-2018-rus.pdf.
4. Кібербезпека: виклики та завдання. [Електронний ресурс] – Режим доступу до ресурсу: https://www.radiosvoboda.org/a/29086067.html.