РОЗДІЛ 1.
ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Виходець Юрій Олександрович

Управління протидії кіберзлочинам в Одеській області Департаменту кіберполіції Національної поліції України, начальник, кандидат юридичних наук

ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ТА ЗАГРОЗИ СТАБІЛЬНОСТІ РОБОТИ КОМП'ЮТЕРНИХ МЕРЕЖ

Будь-кому відомо, що сучасне суспільство є основним генератором інформаційного середовища і повноцінним її споживачем. Базуючись на даному факті, можна з упевненістю говорити про те, що в міру розвитку такого явища, виникають внутрішні безперервні зв'язки і залежності між користувачами глобального, або окремо взятого, інформаційного простору. Починаючи з часів, коли невеликі групи людей стали утворювати племена, поселення, міста, імперії, і закінчуючи сьогоднішнім днем, з плином часу, всередині таких людських, або, якщо говорити про новітній період розвитку суспільства, всередині людино-машинних інфраструктур, почали виникати скупчення інформації, які з тих чи інших причин не розголошувались або не могли бути розголошеними - простіше кажучи, всередині системи обміну інформацією з'явилися секрети. Секрети, або секретну інформацію, людство намагається замаскувати і краще приховати від ворогів ще з часів єгипетських фараонів. Даний період закладає основу процесу побудови комплексу технічних засобів та прийомів, покликаних досягнути необхідного та достатнього рівня забезпечення безпеки в інформаційних мережах. Чим швидше розвивалося суспільство, тим більш витонченими ставали методи контрольованого спотворення інформації - її шифрування. До 19 століття, все шифрування було "ручним", тобто, повністю виконувалося рукою людини. З появою складних обчислювальних механізмів і роторних машин,

частина цього завдання лягла на механізми. Але, коли в життя людства вторглися потужні ЕОМ - комп'ютери, роль людини в цьому процесі звелася до мінімуму і полягала в розробці таких алгоритмів шифрування нового покоління, які давали б можливість так перетворити інформацію, використовуючи потужності обчислювальної техніки, що б ворог жодним чином не зміг її розсекретити. Складність методів і алгоритмів шифрування збільшується прямо пропорційно стрімкому розвитку самих ЕОМ. На сьогоднішній день розроблено безліч алгоритмів шифрування, які в достатній мірі здатні зберегти цілісність і конфіденційність інформації, з огляду на сучасні можливості обчислювальної комп'ютерної техніки. Найбільш популярними алгоритмами в сучасному інформаційному середовищі є симетричні алгоритми - DES, 3DES, AES, - і асиметричні алгоритми, такі як, наприклад, група шифрів RSA зі змінною довжиною ключа.

Концепція захисту даних за допомогою шифрування дуже важлива та має своє місце навіть сьогодні. Так, наприклад, у більшості месенджерів для передачі сигналів та знаків використовується шифрування типу end-to-end, а розробники одного с найбільш захищених месенджерів – Telegram, винайшли свій власний протокол шифрування – MTProto 2.0, який являється яскравим прикладом поєднання декількох алгоритмів шифрування в одне ціле для досягнення найвищого рівня захисту даних.

Шифрування розроблялось для забезпечення потреб в аналізі загроз інформаційної безпеки та дозволяє виділити складові сучасних комп'ютерних загроз - їх джерела і рушійні сили, способи і наслідки реалізації. Аналіз виключно важливий для отримання всієї необхідної інформації про інформаційні загрози, визначення потенційної величини збитку, як матеріальної, так і нематеріальної, і вироблення адекватних заходів протидії. Однією з найбільш розповсюджених загроз кібербезпеки є витік даних (близько 80% кібер-інцидентів).

Однією з найбільших загроз кібербезпеки є можливість однозначного збереження цілісності інформації при зовнішніх або внутрішніх перебоях різноманітного втручання. Для забезпечення захисту від такого типу кіберзагроз

використовують періодичне побітове копіювання інформації з закріпленням контрольних сум масивів даних. Якщо аналізувати ризики та загрози кібербезпеки у 21-му сторіччі, то можна сміливо говорити, що однією з найбільших проблем є проблема «мережевої неграмотності», яка, часто, полягає у не вмінні проектувальників-техніків закривати за собою порти, які, в подальшому, можуть слугувати точками входу для різноманітних програмних засобів або стати майданчиком для заливу «шеллів». «Шелли», в свою чергу, відвантажують до інформаційної системи вихідні коди вірусів-вимагачів - один з видів шкідливого ПЗ. Вони вимагають гроші, блокуючи доступ до файлів або комп'ютерних систем до сплати викупу. При цьому сплата викупу не гарантує відновлення доступу до файлів або системам. Тому, аби вберегтись від можливого зараження системи ШПЗ треба вміти вчасно та зі 100%ю вірогідністю розпізнавати шкідливе програмне забезпечення або сценарій.

Експерти стверджують, що останнім часом спостерігається помітне зростання числа фішингових атак. Ця широко поширена загроза кібербезпеки створює величезний ризик для окремих осіб і організацій. Фішинг атака - це методи, використовувані зловмисниками для крадіжки конфіденційної інформації, коли користувачів намагаються змусити її передати. Більшість користувачів про цю загрозу навіть не підозрюють. Фішинг, як спосіб шахрайства в тій чи іншій формі використовується вже протягом багатьох років. Починався він ще з телефонних дзвінків. Але сьогодні кіберзлочинці розглядають фішинг-атаки як успішний і простий спосіб підготовки більш складних кібер-атак.

З кожним днем користувачі мережі Інтернет створюють все більше інформаційних складових для побудови цілісного інформаційного простору. Однією з таких складових є створення та подальше адміністрування електронних поштових скриньок. Але, масиви таких скриньок зберігаються у величезних контейнерах-серверах, які, в свою чергу вразливі до зламу. В ході отримання хакерами доступу до баз даних велика кількість унікальних пар логін+пароль розміщуються на тіньових майданчиках з метою продажу. Дана загроза кібербезпеки відноситься до типу загроз «несанкціонованого розподілення та

розповсюдження інформації з обмеженим доступом» та виникає у випадку передачі сервісами авторизації або аутентифікації таких даних компаніям, які будують маркетинг на розсилці масових інформаційних повідомлень.

Людина часто стає першою слабкою ланкою при проведенні кібератаки. Виконавець такої атаки після проведення розвідки і вивчення своєї цілі використовує отриману інформацію для входу до облікового запису або інших важливих відомостей, які проведуть його до захищених систем і ресурсів. Найчастіше зловмисникові щастить, і при мінімальних зусиллях і ще меншому ризику з його боку він може дізнатися облікові дані користувача просто на основі припущень, що може бути реалізовано навіть в автоматичному режимі. Тему соціальної інженерії складно обговорювати, тому що багато користувачів надмірно впевнені в своїх здібностях захистити облікові дані і не дотримуються належної «кібергігієни». Це вже призвело до кількох гучних порушень, про які можна докладніше прочитати в Інтернеті.

Говорячи про технічне забезпечення інформаційної безпеки в комп'ютерних мережах можна з впевненістю вказувати на те, що без розробки новітніх шифрів та систем захисту інформації, такий процес є неможливим. В той же час, системи безпеки розробляються безпосередньо людьми, які є найвразливішими до кібер-атак. Враховуючи викладене, можна говорити про те, що технічне забезпечення інформаційної безпеки повинно мати комплексну структуру, яка включає в себе як побудова стресостійких систем, так і проведення відповідної підготовки серед співробітників, які обслуговують такі системи.

Ключові слова: шифрування, інформаційна система, кібер-атака, загроза, зловмисники, захист.

Ключевые слова: шифрование, информационная система, кибер-атака, угроза, злоумышленник, защита.

Keywords: encryption, information system, cyber-attack, threat, attackers, protection.