Комплексний підхід у сфері захисту інформації

Горбатенко Д.С. студент гр. Юс-22 юридичного факультету СумДУ
Науковий керівник - Хворост О.О., к.е.н., викладач кафедри АГП ФЕБ СумДУ

Під захистом інформації слід розуміти використання засобів і методів, вжиття відповідних заходів з метою системного забезпечення необхідної надійності збереженої й оброблюваної інформації.

Слід зазначити, що концепція захисту як система поглядів на цілі, способи забезпечення безпеки інформації і засоби її захисту повинна в загальному вигляді відповідати на три прості питання: що захищати, від чого захищати, як захищати?

Під питанням «що захищати?» мається на увазі набір певних відомостей про об'єкт захисту і перш ніж відповісти на нього, необхідно чітко розібратися, які відомості підлягають захисту.

Питання «від чого захищати?» пов'язане з поняттям «загроза». Загроза - потенційна можливість неправомірного навмисного або випадкового впливу на об'єкт захисту, що приводить до втрати або розголошення секретної інформації.

З питанням «як захищати?» пов'язане поняття «система захисту». Система захисту - це комплекс заходів і засобів, а також діяльність на їх основі, спрямована на виявлення, відображення і ліквідацію різних видів загроз безпеки об'єктів захисту [1, с. 61].

Представники будь-яких суб'єктів господарювання повинні розуміти, що окремі дії з захисту інформації не можуть гарантувати реальну безпеку, а скоріше створюють її видимість. Для дієвого вирішення проблеми необхідні не розрізнені заходи, а професійний системний підхід.

Для обгрунтування актуальності зазначених вище питань, слід вказати, що інститут Ponemon представив результати дослідження, спрямованого на вивчення думки ІТ-та ІБ-фахівців Великобританії, Франції та Німеччини про успішність їхніх компаній в боротьбі з погрозами мережевої безпеки.

Інститутом проведено опитування 1406 ІТ-та ІБ-фахівців Великобританії, Франції та Німеччини, які мають в середньому 10 років досвіду роботи в галузі. Приблизно половина з них займає управлінські і більш високі посади, 42 відсотки працює в компаніях з більш ніж 5000 співробітниками.

Протягом останнього року успішні атаки (один і більше разів) були проведені на 80% компаній.

Половина опитаних не знають, з якого джерела велися атаки.

Половина виявлених атак велася із зовнішніх джерел, 38% виходили від співробітників компаній, 22% - від контрагентів.

Порушення безпеки в основному виникали на робочих станціях або ноутбуках співробітників компанії (44% і 26% відповідно). Причиною 16% атак стали Смартфони і планшети співробітників.

На думку опитаних, найбільш успішний метод протидії злочинцям - комплексний підхід до забезпечення інформаційної безпеки. На 2 і 3 місці за популярністю - доступність ресурсів та наявність перспективних технологій відповідно.

Найбільш серйозними наслідками атак опитані вважають розкрадання інформаційних активів (45%), переривання бізнес-процесів (44%) і санкції з боку регуляторів (27%). Шкоди репутації вказали 10% опитаних [3].

У світовій практиці вже давно використовується таке поняття, як комплексна система захисту, під якою слід розуміти єдину сукупність законодавчих, організаційних і технічних заходів, спрямованих на виявлення, відображення і ліквідацію різних видів загроз безпеки.

Комплексна система захисту дозволяє:за допомогою центральної станції управління проводити збір інформації зі всіх пристроїв ідентифікації та контролю; збирати і обробляти інформацію з обладнання охоронних систем сигналізації, систем відео спостереження, пожежогасіння, вентиляції, енергопостачання та ін; створювати журнали обліку стану цих систем і змін, що відбуваються, демонструвати оператору стан систем та аварійні ситуації в текстовому або графічному вигляді; при підключенні інформаційних каналів, що зв'язують головний об'єкт з філіалами або іншими об'єктами, центральний оператор отримує можливість контролювати стан всієї структури в реальному режимі часу.

Тепер розглянемо етапи здійснення атаки. Перший, підготовчий, етап полягає в пошуку передумов для здійснення тієї чи іншої атаки. На цьому етапі шукаються уразливості, використання яких призводить до реалізації атаки, тобто до другого етапу. На третьому етапі завершується атака, «замітати» сліди і т.д. При цьому перший і третій етапи самі по собі можуть бути атаками. Наприклад, пошук порушником вразливостей за допомогою сканерів безпеки, наприклад SATAN, сам по собі вважається атакою.

Комплексна система забезпечення інформаційної безпеки повинна працювати на всіх трьох етапах здійснення атаки. І забезпечення адекватного захисту на третьому, завершальному, етапі не менш важливо, ніж на перших двох. Адже тільки в цьому випадку можна реально оцінити збиток від «успішної» атаки, а також розробити заходи щодо усунення подальших спроб реалізувати аналогічну атаку.

Враховуючи вимоги сучасного світу до побудови надійної системи захисту, різні організації, такі як, Центр ведення інформаційної війни ВВС США, DISA та інші, на основі методів мережевого управління стали розробляти ефективні підходи до вирішення названих вище проблем.

Ці роботи підхопили й інші компанії, які давно відомі на ринку засобів інформаційної безпеки. До таких компаній можна віднести Internet Security Systems (ISS), Network Associates (NAI), CheckPoint Technologies і т.д. У Росії аналогічні роботи веде НІП «Інформзахист». Кожна компанія-розробник дала свою назву нової технології управління безпекою. Наприклад, ISS назвала свій підхід «моделлю адаптивної мережевої безпеки» (Adaptive Network Security Model, ANSM), компанія NAI своє рішення назвала «активної безпекою» (Active Security), а НІП «Інформзахист» дотримується назви «технологія управління інформаційною безпекою «Беркут». Але суть у всіх цих підходів одна - вони дозволяють забезпечувати захист у реальному режимі часу, адаптуючись до постійних змін в інформаційній інфраструктурі.

В сучасних умовах інформація є одним із найважливіших та найдорожчих ресурсів. У такій ситуації особливо актуального значення набуває задача оцінки імовірності витоку інформації для певного об’єкта і пошуку методів підвищення інформаційного захисту цього об’єкта. Розв’язання цієї задачі традиційними методами пов’язане з цілим рядом труднощів, як економічного, так і психологічного характеру [5].

Отже, захист інформації - це комплексна підсистема організаційно-управлінських, організаційно-технічних та організаційно-правових заходів, засобів, методів, які здійснюються відповідними суб’єктами інформаційних відносин для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованої системи та правомірних користувачів інформацією, яка обробляється, передається і/або зберігається на комп`ютерних носіях (в електронно-цифровому виразі); в разі виникнення делікту (правопорушення) вжиття правового впливу для відновлення реституції попереднього стану, покарання винного і відшкодування завданої матеріальної і моральної шкоди у відповідності з законодавством [6, с. 19].

Література:

1. Правове, нормативне, та метрологічне забезпечення систем захисту інформації в Україні // Матеріали ювілейної науково-технічної конференції. - Київ, 1998 р. с. 61-62
2. Ананський Е.В. Издание публикации Журнал «Служба безопасности», 1999 г. - №11.
3. Украинский интегратор защиты персональных данных: Тенденции сетевой безопасности [електронний ресурс] – Режим доступу: http://www.uipdp.com/articles/2012-09/11.html
4. Лукацький А.В. Адаптивное управление защитой. «Сети. Глобальные сети и телекоммуникации», 1999 г. - №10.
5. Про державну таємницю: Закон України від 21.01.1994 р. // Відомості Верховної Ради України. - 1994 р., № 16, стор. 422, стаття 93
6. Цимбалюк В.С., Гавловський В.Д., Корочанський О.Е. Проблеми юридичної деліктології в інформаційних відносинах \\ Бизнес и безопасность. 1998 г.- № 6 . с.19-21.

Міжнародно-правове забезпечення стабільності та безпеки суспільства : матеріали науково-теоретичної конференції викладачів, аспірантів та студ. юридичного фак-ту, м. Суми, 25 травня 2013 р. / Ред.кол.: А.М. Куліш, М.М. Бурбика, М.І. Логвиненко, В.М. Семенов, А.В. Баранова. — Суми : СумДУ, 2013. — С. 132-134.