СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ВЕБ-ЗАСТОСУНКУ

Земляной О.О., Корнієнко Б.Я.

Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського», Київ, Україна

З широким поширенням застосування мобільних пристроїв і зростання популярності мережевих сервісів виник цілий ряд нових проблем і загроз комп'ютерної безпеки. При цьому частина проблем відноситься до безпеки корпоративних і службових даних, а інша загрожує безпеці особистих даних звичайних користувачів.

Загрози рядовим користувачам можна розділити на кілька категорій: загрози, пов'язані з викраденням персональних даних; загрози цілісності даних; загрози, пов'язані з несанкціонованим використанням належних користувачу комп'ютерних пристроїв і порушенням їх роботи.

Вимоги, що пред'являються до системи захисту інформації

На сьогоднішній день до системи захисту інформації, крім загальної концептуальної вимоги, пред'являються цільові вимоги, які поділяються на:

- економічні (мінімізація витрат на систему, максимальне використання серійних засобів);
- функціональні (забезпечення вирішення необхідної сукупності задач захисту, задоволення всім вимогам захисту);
- технічні (комплексне використання коштів, оптимізація архітектури);
- ергономічні (мінімізація перешкод користувачам, зручність для персоналу системи захисту);
- організаційні (структурованість всіх компонентів, простота експлуатації).

Класифікація способів захисту інформації

В рамках системи безліч і різноманітність видів захисту інформації визначається способами впливу дестабілізуючих чинників (або чинників, що їх породжують) на елементи ІС, інформацію що захищається і навколишнє середовище в напрямку підвищення показників захищеності інформації. Ці

способи можуть бути класифіковані в такий спосіб: морально-етичні та законодавчі, адміністративні та психологічні, захисні можливості програмних і апаратних засобів. Варто не забувати про важливість коректної поведінки самих користувачів, час від часу користувачі повинні міняти паролі, повинні проводитися тренінги з протидії методам соціальної інженерії;

Стани і функції системи захисту інформації

Залежно від подій потенційних впливів загроз і заходів, що знижують їх вплив, система захисту переходить в певні стани, відповідні подіям:

- Стан 1 - захист інформації забезпечений, якщо при наявності умов, що сприяють появі загроз, їх вплив на захищену інформацію було спростовано або ліквідовано наслідки такого впливу;
- Стан 2 - захист інформації порушено, якщо неможливо запобігти впливу на неї загроз, проте вони виявлені і локалізовані;
- Стан 3 - захист інформації зруйнований, якщо результати впливів на неї загроз не тільки не попередили, але і не локалізували.

Безліч функцій захисту інформації визначається наступною послідовністю дій, які забезпечують виконання кінцевої мети - досягнення необхідного рівня інформаційної безпеки. Перш за все, необхідно спробувати попередити виникнення умов, що сприяють появі загроз інформації. Виконання цієї функції в зв'язку з великою кількістю таких загроз і випадковим характером їх проявів має ймовірність, близьку до нуля. Тому наступним кроком має бути своєчасне виявлення проявилися загроз і попередження їх впливу на інформацію. Якщо все-таки такий вплив стався, необхідно вчасно його виявити і локалізувати з метою недопущення поширення цього впливу на всю конфіденційну інформацію, оброблювану на об'єкті. І останньою функцією захисту повинна бути ліквідація наслідків зазначеного впливу для відновлення належного стану безпеки інформації:

- функція 1 - попередження прояву загроз. Реалізація цієї функції носить попереджувальну мету і повинна сприяти такій архітектурно-функціональній побудові сучасних систем обробки та захисту

інформації, яка забезпечувала б мінімальні можливості появи дестабілізуючих факторів в різних умовах функціонування систем;

- функція 2 - виявлення загроз і попередження їх впливу на інформацію. Здійснюється комплекс заходів, в результаті яких загрози повинні бути виявлені до їх впливу на захищену інформацію, а також забезпечено недопущення впливів цих загроз на захищену інформацію в умовах їх прояви;
- функція 3 - виявлення впливу загроз на захищену інформацію і локалізація цього впливу. Зміст функції направлено на безперервний контроль коштів, комплексів, систем обробки та захисту інформації і різних компонентів, що захищаються метою своєчасного виявлення фактів впливу на них загроз. Своєчасне виявлення передбачає забезпечення реальної можливості локалізації впливу на інформацію, тобто мінімізацію можливого порушення її цілісності та захищеності і недопущення поширення цього впливу за межі допустимих розмірів. У комп'ютерних системах, наприклад, цю функцію реалізують апаратно-програмні засоби контролю та реєстрації спроб несанкціонованого доступу в систему або до інформації (цифровий підпис);
- Функція 4 - ліквідація наслідків впливу загроз. Функція передбачає проведення заходів захисту щодо виявленого і локалізованого впливу загроз на інформацію, тобто здійснюється відновлення системи.

Захищеність системи

Захищеність самої системи може бути підвищена за рахунок виконання певних конфігураційних налаштувань на машині, де фізично розгорнуто додаток:

- надійний пароль користувача admin з регулярним оновленням;
- рольова модель доступу до додатків;
- криптографічна верифікація пакетів;
- використання ключів для з'єднання по протоколу SSH;

- шифрування диска;
- автоматичне оновлення налаштувань безпеки від постачальника операційної системи.

Література

1. Корнієнко Б.Я. Дослідження імітаційного полігону захисту критичних інформаційних ресурсів методом IRISK. Моделювання та інформаційні технології. 2018. Вип. 83. С. 34-41.
2. Корнієнко Б.Я. Побудова та тестування імітаційного полігону захисту критичних інформаційних ресурсів. Наукоємні технології. 2017. № 4 (36). С. 316 - 322.
3. Korniyenko B., Yudin A., Galata L. Risk estimation of information system.Wschodnioeuropejskie Czasopismo Naukowe. 2016. № 5. P. 35 - 40.
4. Корнієнко Б.Я., Юдін О.К., Снігур О.С.Безпека аутентифікації у web-ресурсах. Захист інформації. 2012. № 1 (54). С. 20 -25. DOI: 10.18372/2410-7840.14.2056 (ukr).
5. Корнієнко Б.Я., Максімов Ю.О., Марутовська Н.М. Прикладні програми управління інформаційними ризиками. Захист інформації. 2012. № 4 (57). С. 60 – 64. DOI: 10.18372/2410-7840.14.3493 (ukr).
6. Galata, L., Korniyenko, B., Yudin, A.: Research of the simulation polygon for the protection of critical information resources. In: CEUR Workshop Proceedings, Information Technologies and Security, Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security (ITS 2017), 30 Nov 2017, Kyiv, Ukraine. vol. 2067. pp. 23–31., urn:nbn:de:0074-2067-8.
7. Корнієнко Б.Я. Безпека інформаційно-комунікаційних систем та мереж. Навчальний посібник для студентів спеціальності 125 «Кібербезпека». – К.:НАУ, 2018. – 226 с.
8. Корнієнко Б.Я., Галата Л.П. Оптимізація системи захисту інформації корпоративної мережі. Математичне та комп'ютерне моделювання. Серія: Технічні науки, Випуск 19, 2019. - С. 56-62.
9. Korniyenko B., Galata L. Implementation of the information resources protection based on the CentOS operating system. Conference Proceedings of 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON - 2019) July 2 – 6, 2019, Lviv, Ukraine. - pp. 1007-1011.
10. Галата Л.П., Корнієнко Б.Я., Заболотний В.В. Математична модель протидії загрозам у системі захисту критичних інформаційних ресурсів. Наукоємні технології, Том 43, № 3, 2019. – С. 300 – 306.

11. Корнієнко Б.Я. Modeling of information security system in computer network. Безпека інформаційних систем і технологій, Том №1 (1), 2019. – С.36-41.

12. Korniyenko B., Galata L., Ladieva L. Research of Information Protection System of Corporate Network Based on GNS3. Conference Proceedings of 2019 IEEE Inernational Conference on Advanced Trends in Information Theory (IEEE ATIT - 2019) Dezember 18 – 20, 2019, Kyiv, Ukraine. - pp. 244-248.

13. Korniyenko B., Galata L., Ladieva L. Mathematical model of threats resistance in the critical information resources protection system. CEUR Workshop Proceedings, Selected Papers of the XIX International Scientific and Practical Conference "Information Technologies and Security" (ITS 2019) Kyiv, Ukraine, November 28, 2019. Vol-2577. P.281-291.

14. Корниенко Б.Я. Кибернетическая безопасность – операционные системы и протоколы. ISBN 978-3-330-08397-4, LAMBERT Academic Publishing, Saarbrucken, Deutschland. − 2017. – 122 с.

15. Korniyenko B.Y., Galata L.P. Design and research of mathematical model for information security system in computer network. Наукоємні технології. – 2017, № 2 (34), С. 114 - 118.

16. Корниенко Б.Я. Информационная безопасность и технологии компьютерных сетей : монография. ISBN 978-3-330-02028-3, LAMBERT Academic Publishing, Saarbrucken, Deutschland. − 2016. – 102 с.

17. Korniyenko B., Galata L., Kozuberda O. Modeling of security and risk assessment in information and communication system. Sciences of Europe. – 2016. – V. 2. – No 2 (2). – P. 61 -63.

18. Korniyenko B. The classification of information technologies and control systems. International scientific journal. – 2016. –№ 2. – P. 78 - 81.

19. Корнієнко Б.Я. Інформаційні технології оптимального управління виробництвом мінеральних добрив :монографія. – К.: Вид-во Аграр Медіа Груп, 2014. – 288 с.

20. Korniyenko B., Galata L., Ladieva L. Security Estimation of the Simulation Polygon for the Protection of Critical Information Resources / B. Korniyenko, //CEUR Workshop Proceedings, Selected Papers of the XVIII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2018) Kyiv, Ukraine, November 27, 2018, Vol-2318, - P. 176-187, urn:nbn:de:0074-2318-4