9. Дослідження основних підходів захисту веб орієнтованих інформаційних систем

Лідія Власенко, Сергій Грибков
Національний університет харчових технологій, Київ, Україна

Вступ. Розвиток Індустрії 4.0 вимагає від сучасних підприємств постійно вдосконалювати корпоративні інформаційні системи та організації доступу до них через Інтернет для підвищення якості управління. Одним з актуальних напрямків розвитку та удосконалення веб орієнтованих інформаційних систем є забезпечення інформаційної безпеки, яка полягає у збалансованому захисті конфіденційності, цілісності та доступності даних, з урахуванням доцільності застосування і без будь-якої шкоди продуктивності організації. Тому необхідно виділити основні підходів захисту веб орієнтованих інформаційних систем.

Матеріали і методи. Теоретичною основою роботи є наукові роботи провідних вітчизняних і зарубіжних вчених в області побудови та підтримки захисту веб орієнтованих систем.

Результати. Для реалізації надійного захисту корпоративних даних при створенні та удосконаленні інформаційної системи необхідно чітко виділити дані, що потребують захисту, та коло робітників, які мають до них доступ. Також, необхідно виділити дані з обмеженим доступом, що мають службову таємницю. Таким чином на етапі проєктування та створення необхідно застосовувати інструменти та методи для усунення більшості недоліків у захисті.

До одних з основних підходів захисту відносять обрання хостингу для розміщення веб системи чи сайту, адже більшу частину задач захисту забезпечить представник послуг, наприклад: управління базами даних; налаштування прав доступу; відновлення резервних копій; наявність функцій автоматичного встановлення CMS; забезпечення автоматичного архівування. У разі використання власного сервера використовують міжмережевий екран нового покоління (NGFW - next generation firewall) для запобігання вторгненням та фільтрації трафіку для додатків (WAF - web application firewall). NGFW контролює доступ зовнішніх додатків до даних підприємства, а WAF захищає користувацькі додатки на внутрішніх серверах, аналізуючи дані, що передаються за протоколами HTTP та HTTPS. Наступним кроком є використання SSL-сертифікатів, які генерується безкоштовно. Постійно необхідно проводити аналіз захисту свого ресурсу тестами на проникнення, в тому числі на SQL-ін'єкції. Навіть перевірка безкоштовними онлайн сервісами можна забезпечити високий рівень захисту. До найпоширенихонлайн сервісів доцільно віднести наступні: Approof от Positive Technologies – перевіряє конфігурацію веб-налаштування, виявляє вразливі компоненти, незахищені дані та шкідливий програмний код; SecurityHeaders.io – перевіряє наявність та коректність заголовків відповіді сервера, які забезпечують безпеку веб-додатків; Observatory by Mozilla – сканує ресурс на наявність проблем безпеки та аналізує захист в цілому; SSL Server Test – виконує аналіз SSL-конфігурації веб-сервера; ASafaWeb – виявляє наявність вразливості конфігурації сайті побудованих на ASP.NET; Snyk – сканує JavaScript, Ruby и Java-додатки на наявність проблем безпеки, а також пропонує їх усунення.

Висновки. За результатами дослідження було виділено основні підходи захисту веб орієнтованих інформаційних систем, які доцільно використовувати при створенні, удосконаленні та супроводі сучасних веб орієнтованих корпоративних систем, що відповідають сучасним тенденціям розвитку Індустрії 4.0.