УДК 004.056
О. Ревнюк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЯКІСТЬ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЙ

UDC 004.056
Revnuk O.

THE QUALITY OF INFORMATION SECURITY MANAGEMENT OF ORGANIZATIONS

За останнє десятиліття організації прагнули стати більш ефективнішими та продуктивнішими шляхом впровадження інформаційних та комунікаційних технологій на свої рішення. Технології стають все більш поширеними, їхня внутрішня цінність стає нижчою порівняно з критично важливою інформацією, яку вони опрацьовують. Такий тісний зв'язок між технологіями та бізнес-функціями виявився двигуном для різкого збільшення інцидентів і збоїв у сфері інформаційної безпеки, що призводить до значних витрат компанії. Відповідно організації краще усвідомлюють ризики інформаційної безпеки та потребу вживати відповідних заходів. Однак з такою кількістю доступних варіантів безпеки багато організацій намагаються визначити найкращі способи протидії загрозам, з якими вони стикаються.

Прагнучи захистити конфіденційність, цілісність і доступність бізнес-процесів, галузь інформаційної безпеки демонструє різноманітні набори продуктів, послуг, процесів і політик, починаючи від складних математичних алгоритмів шифрування до управління людськими ресурсами та законодавством [1]. Оскільки власники компаній не впевнені в найкращому контролі безпеки для своїх продуктів – часто розгортають якомога більше засобів захисту, незважаючи на їхню якість чи ефективність.

Насамперед організації повинні підвищувати якість шляхом раціонального впровадження засобів контролю, необхідних для мінімізації дефектів і забезпечення безперервної функціональності бізнесу. Завдяки більш точному розумінню практики управління інформаційною безпекою можна зрозуміти, яким чином застосовувати ефективні стратегії для покращення якості та зниження ризику.

Багато перших програм інформаційної безпеки покладалися в значній мірі на технологічні інновації. Такий підхід був доцільним, оскільки багато активів, які потребували захисту, також були високоякісними технологічно. При правильному використанні ці методи значно зменшують вірогідність атаки на безпеку в веб-додатках.

Однак, якими б успішними та складними не були ці технології, лише технічні підходи не можуть вирішувати проблеми безпеки з тієї простої причини, що безпека інформації – це не просто технічна проблема. Це також соціальна та організаційна проблема [2]. Національний інститут стандартів і технологій США класифікує засоби контролю інформаційної безпеки на три групи:

- Технічний контроль – традиційно включає продукти та процеси (такі як брандмауери, антивірусне програмне забезпечення, виявлення вторгнення та методи шифрування), які фокусуються в основному на захист програмного забезпечення організації та інформації, що обробляється в системі.
- Операційний контроль – включає механізми та способи усунення недоліків роботи, які можуть використовувати різні загрози; контроль фізичного доступу, можливості резервного копіювання.
- Контроль управління – політика використання, навчання співробітників та планування безперервності роботи бізнесу спрямовані на нетехнічні сфери інформаційної безпеки.

Основною метою є визначення засобів контролю, які організації в середньому впроваджують комплексно порівняно з елементами контролю, які впроваджуються погано.

Віруси та шкідливий код є одними з більш очевидних ризиків стійкості засобів безпеки, тому більшість організацій старанно захищаються від загроз, які вони створюють. Часто, веб-сайти та програмне забезпечення оснащені резервним копіювання інформації та надійним управленням системи, що є теж досить вагомим плюсом в якості управління інформаційною безпекою[3]. Також організації зосереджені щодо технічної документації, принаймні в області розробки та підтримки свого продукту.

Проте є і погані риси захисту інформації, які притаманні багатьом компаніям. Погано реалізоване навчання персоналу для запобігання атакам соціальної інженерії, особливо тих, хто має доступ або знання до систем, що містять конфіденційну інформацію. Такі люди є потенційними жертвами атак соціальної інженерії. Організації також повинні вміти виявляти інциденти та усувати їх загрози.

Також важливо виявляти загрози в режимі реального часу і у разі порушення безпеки – система повинна сповістити відповідних осіб для реагування. Нажаль це правило часто нехтується. Організації, які мають системи виявлення загроз веб-додатків без реального часу сповіщення – схожі на будинки, наповнені детекторами диму, які не мають механізмів сигналізації. [4]

Організації повинні усвідомити, що значна частина проблем інформаційної безпеки виходить далеко за межі технологій. Навчитися оцінювати роль менш технічних засобів контролю, таких як розробка політики безпеки – грає велику роль для мінімізації ризиків здійснення атак на систему.

Впровадження всіх доступних елементів керування та захисту не є ефективним використанням ресурсів, тому організації повинні інвестувати в безпеку лише до точки, коли гранична вигода дорівнює граничній вартості. Цей принцип стосується як компанії в цілому – так і кожного працівника окремо. Можна, наприклад, оптимізувати рентабельність інвестицій, запровадивши три засоби керування на середньому рівні, а не один комплексний рівень.[5]

Сучасні організації активно прагнуть контролювати інформаційну безпеку, але вони стараються досягнути певних цілей істотно різними шляхами. Загалом, багато організації керують безпекою дещо непослідовно та поверхово. Замість того, щоб використовувати прорахований чи раціональний підхід, вони наголошують на певних елементах керування, залишаючи інші, хоча й не менш важливі, погано захищеними.

Кожній компанії слід додатково дослідити переваги поєднання різних рівнів технічного, управлінського та операційного засобів керування для досягнення справжньої цілісної безпеки від різноманітних поточних і майбутніх ризиків.

Література

1. O.S. Saydjari, «Multilevel Security: Reprise,» IEEE Security & Privacy. Vol. 2. No. 5. 2004. P. 64–67.
2. R.T. Mercuri, «Computer Security: Quality Rather than Quantity,» Comm. ACM. Vol. 45. No. 10. 2002. P.12–14.
3. D.W Straub and R.J. Welke, «Coping with Systems Risk: Security Planning Models for Management Decision Making,» MIS Quarterly. Vol. 22. No. 4. 1998. P. 441–470.
4. G. Dhillon and J. Backhouse, «Information Systems Security Management in the New Millennium,» Comm. ACM. Vol. 43. No. 7. 2000. P. 125–128.
5. G. Stoneburner, A. Goguen, and A. Feringa, «Risk Management Guide for Information Technology Systems,» Nat'l Inst. of Standards and Technology, US Dept of Commerce. 2002. URL: http://csrc.nist.gov/publications/nist pubs/800-30/sp800-30.pdf.