Шишола І.М.
студент,
Навчально-науковий інститут захисту інформації
при Національній академії Служби безпеки України

ПЕРЕВАГИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ТА ЗАХИСТУ ІНФОРМАЦІЇ

З розвитком нових технологій в різних областях виникли загрози безпеки інформації, що зберігається в багатьох організаціях. Кібербезпека – це захист систем в організаціях, їх даних і мережі в кіберпросторі. На сьогодні більшість керівників підприємств розуміють, що кібербезпека є важливою складовою для успішного функціонування підприємств, особливо тих, що працюють з базами даних клієнтів та/або з особисто розробленими технологіями. У бізнесі або будь-якій організації, існують різні загрози, пов'язані з їхніми системами, даними і мережами. Задля аналізу та знаходження необхідного методу з метою досягнення кібербезпеки, розглянемо основні аспекти використання захисту інформації та інформаційного забезпечення.

Існує багато переваг захисту інформації, включаючи дотримання нормативних стандартів, запобігання дорогим інцидентам безпеки, підтримання репутації бізнесу та збереження довіри клієнтів, постачальників, партнерів та акціонерів. Неспроможність захистити конфіденційну інформацію може призвести до штрафів, виданих регулюючими органами, або судових позовів від інших компаній або фізичних осіб, якщо вони зазнають негативних наслідків, що були спричинені внаслідок порушення зберігання їх особистих даних.

Забезпечення інформацією також пропонує багато переваг на додаток до тих, що забезпечуються захистом інформації. На додаток до безпеки, гарантія інформації ще й забезпечує цілісність даних, зручність використання, відмову від достовірності та автентичність. Досягається конфіденційність, а також доступність та надійний і своєчасний доступ до інформації.

Першочерговим у використанні будь-якого методу захисту інформації керівна ланка підприємства має здійснити оцінку кібер-ризику. Це крок, який має бути першим при прийняті рішення компанії щодо збереження цілісності інформації. Етап оцінки ризику – це ідентифікація активів різних організацій, на які може вплинути шахраї, бази даних та інше обладнання, що містить основні дані. Після ідентифікації потенційних ризиків наступним кроком є вибір систем управління для запобігання нападу.

Розглянемо як працює охорона інформації та інформаційного забезпечення для оцінки ефективності у використанні кожного.

Захист інформації стосується зменшення ризиків через безпечні системи та архітектуру, які усувають або зменшують вразливість. ІР має справу як з операціями, так і з технологіями, щоб спробувати створити успішний метод усунення будь-яких уразливих «точок» системи, які можуть бути використані для отримання несанкціонованого доступу або компромісу чи крадіжки даних. Вона може включати такі аспекти, як керування вразливими «точками»,

тестування проникнення та технологічних рішень, такі як брандмауери, антивіруси, запобігання втраті даних та шифрування.

Забезпечення інформації визначає способи більш ефективного контролю та захисту критично важливої інформації, підкреслюючи управління організаційними ризиками та загальну якість інформації. Забезпечення інформації, як правило, є більш широкою стратегічною ініціативою, що складається з широкого спектру процесів захисту інформації та управління. Прикладами можуть бути перевірки безпеки, архітектура мережі, аудит відповідності, управління базами даних, розробка, впровадження та забезпечення реалізації політик управління організаційною інформацією.

Проаналізуємо найкращі практики захисту інформації та інформаційного забезпечення.

Крок перший для впровадження успішної програми захисту інформації та забезпечення інформації – признання керівництвом компанії, що обидва з тих, що ми розглядаємо, є життєво важливими для загального стану бізнесу та його прибутковості.

При розробці та впровадженні програм захисту інформації або забезпечення інформації варто ознайомитися з існуючими найціннішим практиками та методиками, які опубліковані в різних організаціях для орієнтування. Методологія оцінювання інформаційної безпеки (INFOSEC) Агентство національної безпеки (NSA) включає 18 базових категорій, які повинні бути присутніми в позиції забезпечення інформації, включаючи такі елементи, як ідентифікація та аутентифікація, контроль сеансу, аудит, управління конфігурацією, маркування, резервування даних, визначені ролі та обов'язки, захист від вірусів, планування на випадок надзвичайних ситуацій та багато іншого – включаючи програми навчання та підвищення обізнаності персоналу, що є, зазвичай, недооціненим, але критичним компонентом захисту інформації та забезпечення інформації.

Кінцевою метою захисту інформації та забезпечення інформації є підтримка цілісності, надійності та доступності даних. Це включає в себе запобіжні заходи проти несанкціонованого знищення або зміни інформації та забезпечення відмови та достовірності даних. Ці зобов'язання забезпечать надійний і своєчасний доступ до даних, зберігаючи конфіденційність і безпеку, та повинні бути пріоритетними для організацій.

Підсумовуючи, зазначимо, що існують також і певні основи, які допоможуть при здійсненні організації кібербезпеки на підприємстві. Ці основи включають управління людьми, процесами і технологіями. Беручи до уваги управління людьми, необхідний штат, професійні навички та кваліфікації, а також складові ресурси. Управління процесами включає IT аудит, управління системами, механізми та практики їх використання. Але останнім фундаментом є технологія, і вона включає процес компетентності та підтримки. Інтеграція трьох основних підходів до кібербезпеки це те, що робить організацію кіберзахищеною. Технологія є первинним елементом у досягненні найбільш ефективної кібербезпеки. Програми кібербезпеки включають використання антивірусних програм, антишпигунських програм і шифрування даних.