УДК 004.6
Ковальчук І. – ст.гр.СТм-51
Тернопільський національний технічний університет імені Івана Пулюя

ПРИНЦИПИ ПРОЕКТУВАННЯ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Kovalchuk I.
Ternopil Ivan Puluj National Technical University

PRINCIPLES OF DESIGNING PROTECTED INFORMATION SYSTEMS

Здебільшого розробники та аналітики добре усвідомлюють і щиро стурбовані безпекою інформаційних систем. Джордж Ву [1] та Макбет [2] вважають, що бувають випадки, що вони не виявляють своєї занепокоєності шляхом включення спеціальних заходів контролю в системи, які вони створюють, покращують і обслуговують.

Відповідно до досліджень Чарльза Вуда [3] - це відбувається, коли не вистачає: фінансування, освічених розробників та досвідчених спеціалістів з інформаційної безпеки чи інших сторін, які розуміють, як інтегрувати елементи керування в систему, поки вона все ще розробляються.

Причина цього полягає в тому, що їм не вистачає знань про принципи проектування безпечних інформаційних систем, які можна використовувати при виборі або розробці заходів контролю. Вони будуть сприяти процедурі побудови засобів контролю безпеки – згідно публікації Алана Бріла. [4]. Відповідно до ідей, котрі просуває Чарльз Вуд [6] та Філіп Кропаткін [5], можна описати наступні ключові принципи проектування захищених інформаційних систем.

Простота - чим менш складним є засіб керування, тим менше зусиль буде витрачено на його проектування, впровадження, функціонування тощо. Це, у свою чергу, підвищить ймовірність того, що він буде економічно ефективним. Користувачі та менеджери хочуть виконувати свою роботу, а не витрачати час на заходи контролю. Відповідно, тим ефективнішим є контроль, чим менше залежить від людей у реальному часі. У багатьох випадках простіші засоби керування є сильнішими за складні, тому що їх можна ретельно зрозуміти й перевірити.

Принцип найменшого привілею - передбачає те, що військові називають « що потрібно знати». Це вказує на те, що доступ до інформації, здатність виконувати певні програми та інші системні привілеї повинні бути обмежені тими, хто може продемонструвати або аргументувати потреби, пов’язані з бізнесом або місією. Найменший привілей є дуже потужним принципом безпеки, але надмірне використання має значні побічні ефекти. Наприклад, якщо співробітники не знають, що роблять інші або як вони це роблять, у них буде мало можливостей внести пропозиції щодо покращення діяльності організації. [5]. Незалежність контролю проявляється в тому, що особа, якій доручено розробляти, впроваджувати та керувати контролем, не повинна бути тією самою особою, яка контролюється таким чином. В цьому випадку існував би конфлікт інтересів, оскільки особа, яка впроваджувала систему контролю, водночас контролюється цією системою [5].

Підзвітність є одним із найбільш фундаментальних принципів внутрішнього контролю для безпеки інформаційних систем. Виконання заходів контролю має бути покладено на конкретних осіб, тобто принаймні одна особа має чітко нести відповідальність за належне функціонування контролю. Наприклад, призначення відповідальності за використання певного ідентифікатора користувача кожній особі, якій видано ідентифікатор користувача, є важливою частиною забезпечення того,

щоб користувач не повідомляв свій пароль, не вибирав пароль, який легко вгадати, або інакше поводитись таким чином, що ставить під загрозу безпеку, яку забезпечують пакети керування доступом на основі пароля.[5]

Принцип найменш загального механізму, який спрямований на мінімізацію залежності від інших компонентів центральної системи, які можуть стати недоступними. Принцип вказує на те, що системи повинні мінімізувати кількість механізмів, які спільно використовують різні користувачі, для їхньої взаємної безпеки.[5]. Принцип участі людини вимагає посередництва людини в кожному критичному чи дуже важливому рішенні. Хоча в області штучного інтелекту, експертних систем, нейронних мереж та інших «розумних машин» було зроблено вражаючі кроки вперед, не слід повністю покладатися на всемогутність і комплексне бачення програмування, що стоїть за цими системами. Неминуче виникнуть обставини, коли відповідь, надана машиною, буде неправильною, непридатною або ненадійною. Комп'ютерні системи не можуть оцінити всі можливі обставини і не можуть розраховувати на здоровий глузд. Відповідно, завжди має бути людина, яка виконує функцію подвійної перевірки системи. [5]. Принцип ревізійності - вимагає, щоб засоби контролю створювали достатні докази того, що вони працювали правильно. Ці докази можуть мати форму журналів, контрольних журналів, звітів або інших форм явного чи прихованого зворотного зв'язку. Одним із найяскравіших прикладів є системи контролю доступу на основі паролів, які можуть генерувати об'ємні журнали, що показують, коли користувачі ввійшли в систему, коли вони вийшли, програми, які вони запускали, і запити на доступ, які вони надіслали (схвалені чи відхилені). Без доказів того, що контроль працює належним чином, керівництво не може бути впевненим що контроль насправді виконує роботу, для якої він призначений. Без таких доказів керівництво не в змозі внести корективи, щоб контроль краще виконував свою роботу. [5]

Дуже рідко всі описані вище принципи керування застосовні до будь-якої системи, що розробляється, вдосконалюється або підтримується. Проте, вивчивши та зрозумівши, як ці принципи можуть бути застосовані до запропонованої конструкції системи, розробник, ймовірно, згенерує багато ідей для покращення інформаційної безпеки. Зберігаючи відкритий розум і не відкидаючи відразу принципи контролю, розробник зможе створити ще більшу кількість пропозицій щодо покращення безпеки – вважає Філіп Кропаткін і Річард П. [5]

Деякі з вищезгаданих принципів можуть вказувати на суперечливі конструкції систем. Це не повинно викликати занепокоєння або втрати довіри до принципів; натомість це доказ реальної потреби приймати рішення щодо компромісів. Надійні системи складаються з добре спроектованої тканини багатьох елементів керування, які, загалом, працюють разом синергетично. Справжнє завдання для розробника інформаційнї систем полягає в тому, щоб зрозуміти синергетичні, антагоністичні та симбіотичні відносини між елементами керування та включити це розуміння в систему.[4][5]

Література.

1. Джордж Ву. Інформаційні та комунікаційні технології для цілей сталого розвитку: сучасний стан, потреби та перспективи / Джордж Ву. - IEEECcommun. Опитування Tuts., вип. 20, № 3, стор. 2389–2406, 3 квартал, 2019.
2. С. Макбет, Самоорганізуюче управління даними та знаннями, створеними користувачами / С. Макбет. - IEEECcommun, вип. 30, № 3, стор. 237–264, травень 2018 р.
3. Чарльз Крессон Вуд. Процедура захисту корпоративних інформаційних систем / Чарльз Вуд – Лондон: Комп'ютери і безпека, 2015.
4. Алан Е. Бріл. Вбудовування засобів керування в структуровані інформаційні системи / Алан Е. Бріл. – Нью-Йорк: Yourdon Press, 2016.
5. Філіп Кропаткін. Принципи управління для захисту активів / Філіп Кропаткін, Річард П. Куссеров. – Нью-Йорк: Yourdon Press,,2015.
6. Чарльз Крессон Вуд. Комп'ютерна безпека: комплексний контрольний перелік елементів керування/ Чарльз Крессон Вуд - Нью-Йорк: John Wiley & Sons, 2017.