готовності інформаційно-комунікаційних технологій до забезпечення безперервності бізнесу».

Стандарт ISO/IEC 27031 встановлює вимоги до ІСТ з метою забезпечення безперервності бізнесу, що дозволяє організаціям бути готовими до таких інцидентів, як кібер-атаки, і застосовувати системи ІСТ резервного копіювання, які будуть копіювати у найкоротші терміни. Цей стандарт пов'язаний з рядом інших міжнародних стандартів на процеси налаштування готовності системи до інцидентів, планування відновлення після збоїв, а також реагування на надзвичайні ситуації та управління. Цей ряд охоплює:

- стандарт ISO/IEC 27035, який встановлює вимоги до управління інформаційною безпекою під час інциденту;
- стандарт ISO/IEC 24762, який надає настанови стосовно засобів відновлення у разі пошкодження ІСТ;
- стандарт ISO/IEC 18043, який встановлює вимоги до вибору, впровадження та функціонування системи виявлення вторгнень (IDS);
- стандарт ISO/IEC 27010, який встановлює вимоги до управління інформаційною безпекою міжсекторного зв'язку;
- стандарт ISO/PAS 22399:2007, який надає настанови щодо забезпечення готовності до інциденту і оперативного управління безперервністю у діяльності;
- стандарт ITU-T X. 1056, який встановлює вимоги до управління безпекою під час інцидентів та надає настанови для телекомунікаційних організацій.

Разом із стандартами серії ISO/IEC 27001 ці стандарти надають набір інструментів управління для визначення різниці між виживанням і руйнуванням бізнесу організації. Ці стандарти підвищують здатність організації до зменшення впливу більшості кібер-атак.

Бізнес-середовище постійно змінюється, разом з ним змінюються й потенційні загрози для виживання компаній. Організації мають постійно бути попереду гри. Належний захист може бути побудований на основі управління ризиком ISMS відповідно до вимог стандарту ISO/IEC 27001 та готовності до інцидентів і управління безперервністю бізнес-процесів на основі стандартів ISO/IEC 27031 та ISO/IEC 27035.

Ризики існують завжди, адже організації використовують однакові технології та програми, спілкуються через мережу Інтернет, отже, бути підготовленим — це просто здоровий глузд.

Охорона платежів. Стандарти ISO посилюють захист у мережевому світі

Джон Ф. Шітс[7]

Стандарти у сфері платежів та у сфері безпеки платежів є наріжним каменем системи роздрібних платежів. Технічний комітет ISO/TC 68 «Фінансові послуги» розробляє стандарти, які є важливими для забезпечення миттєвого виконання мільярдів транзакцій на трильйони доларів.

Без стандартів ISO та платіжних систем, розроблених відповідно до вимог цих стандартів, власник картки з Кігалі, Руанда, не зможе швидко, зручно і безпечно оплачувати товари та послуги під час поїздки до Парамарібо, Сурінам. Більш того, без стандартів ISO в галузі безпеки фінансові установи з усього світу не змогли б побудувати глобальну систему співробітництва та багатомільярдну платіжну систему за допомогою карток.

[7] Джон Ф. Шітс, керівник робочої групи ISO/TC 68/SC 2/WG 13 «Безпека роздрібної банківської справи» та голова американської робочої групи ASC X9 F6 «Перевірка справжності картки і ICCs». Він протягом 25 років працював у сфері платежів, а зараз є старшим бізнес-керівником, відповідальним за розроблення технології оплати для Visa, Inc.

Багато стандартів ISO в сфері безпеки роздрібних фінансових платежів зосереджують увагу на захисті персонального ідентифікаційного коду (PIN), який підтверджує право людини використовувати конкретну платіжну картку. Цей код є коротким для легкого запам'ятовування, в результаті чого може бути легко викраденим, якби не цілий ряд вимог до кодифікування та заходів безпеки, встановлених стандартами ISO. Стандарти охоплюють вимоги до:

- пристроїв опрацювання та приймання PIN-кодів;
- логічного захисту PIN-кодів за допомогою шифрування;
- управління ключами шифрування для захисту PIN-кодів;
- ідентифікації повідомлення щодо операції задля підтвердження її автентичності та цілісності;
- форматів повідомлень та протоколів повідомлень щодо операції.

Проти усіх загроз безпеці

Сьогодні існують нові, досконаліші алгоритми шифрування, однак їхнє упровадження не є простим відключенням старих і підключенням замість них нових алгоритмів шифрування. Навпаки, повинні бути ретельно розглянуті та проаналізовані вимоги безпеки та функціонального призначення з метою забезпечення впевненості у тому, що новий алгоритм повністю забезпечить очікування користувачів та усуне будь-які випадковості.

Одним із доказів того, наскільки важливими є ці процеси, є досвід останнього переведення галузі з старого на нові алгоритми шифрування, який відбувався 10 років тому. На ранній стадії упровадження нових алгоритмів шифрування вони були майже в 36 квадрильйонів разів менш ефективними, ніж планувалося. Завдяки змінам, що були прийняті за допомогою стандартизації та спрямовані на усунення недоліків і безпечне впровадження, нові алгоритми шифрування сьогодні ефективно працюють.

PIN-коди є статичними показниками, а тому мають бути захищені скрізь, де їх використовують, опрацьовують або зберігають. Оскільки PIN-коди піддаються ризикам шахрайства, платіжний бізнес шукає нові методи ідентифікації, які встановлюють автентичність не через незмінні показники, а використовуючи ідентифікаційні коди, що динамічно генеруються і можуть бути використані тільки для однієї транзакції, що зменшить вірогідність шахрайств.

Нові можливості платежів

Хоча використання і захист PIN-кодів залишається важливою темою для існуючих та нових стандартів ISO, разом з ними розробляють стандарти для вирішення проблем торгівлі та шахрайства. Велика частина цієї роботи залишається для попередньої стандартизації, але технічні звіти ISO (TRs) є настановами для розроблення нових технологій.

Захист PIN-кодів у відкритому мережевому оточенні є серйозною проблемою, оскільки до мережі Інтернет підключені сотні мільйонів пристроїв. Відповідні настанови ISO щодо безпечного прийняття в цьому просторі попереджають, що PIN-коди ніколи не повинні бути введені в пристрої загального призначення для передавання через Інтернет. Якщо PIN-коди використовуватимуть у цьому середовищі, то їх мають використовувати виключно у поєднанні з картами на інтегральній схемі (ICCs) і відправляти на карту для перевірки.

Основою для розроблення сучасних стандартів на фінансові повідомлення є стандарт ISO 8583 на процеси передавання та формат фінансових повідомлень систем опрацювання даних платіжних карт 20-річної давнини. Розроблення універсальних стандартів на обмін фінансовими повідомленнями є складним і трудомістким процесом, під час реалізації якого можуть виникнути різні проблеми.

Основною причиною збоїв у протоколах безпеки є проблеми взаємодії, що впливають на ефективність роботи, а тому під час розроблення цієї нової структури платежів необхідно враховувати вимоги всіх зацікавлених сторін.

Стандарти мають відповідати потребам тієї конкретної галузі, для якої вони були розроблені, що може призвести до розробляння багатьох стандартів, які стосуються однієї теми або декількох дуже близьких. Прикладом цього є стандарт ISO/IEC на безпеку в галузі IT та аналогічні стандарти, розроблені технічним підкомітетом ISO/TC 68/SC 2. Стандарти ISO/IEC на безпеку IT забезпечують широкий, узагальнений набір вимог безпеки для IT-систем. Одночасно стандарти, розроблені технічним комітетом ISO/TC 68, мають посилання на ці стандарти безпеки, при цьому не існує і не повинні розроблятись стандарти ISO/IEC IT для конкретних потреб ринку фінансових послуг.

Чималу кількість необхідних вимог безпеки для фінансового світу розглядатимуть як зайві в світі IT-середовища. Таким чином, упровадження стандартів ISO/IEC на безпеку у сфері IT часто буває недостатнім для захисту фінансових транзакцій.

Сучасні процеси стандартизації забезпечують розгляд потреб усіх зацікавлених сторін, а стандарти забезпечать функціональність та безпеку, яких вимагає нинішній світ. Метою процесу стандартизації є своєчасність розроблення стандартів та їхня актуальність у мінливому світі. ■

(За матеріалами Інформаційного бюлетеню з міжнародної стандартизації, №3'2011)