Три додатки до стандарту ISO 28004 було розроблено після публікації стандарту з метою надання додаткових корисних рекомендацій:

Amd 1 призначений для виконання середніх та малих операцій підприємствами морського порту (на підтримку прохання Міжнародної морської організації (IMO)).

Amd 2 надає конкретні настанови малим і середнім підприємствам (SMEs) щодо впровадження стандарту ISO 28000.

Amd 3 надає конкретні настанови організаціям, які прагнуть виконувати вимоги стандарту ISO 28001. Настанови щодо убезпечення, вміщені до стандарту ISO 28001, детально розроблено у співпраці зі Світовою митною організацією (WCO). Опублікований як PAS у 2010 році.

Стандарт ISO 28005 *«Системи управління безпекою ланцюга постачання. Портові операції з використанням електронних систем (EPC)»*. Цей стандарт розроблений відповідно до вимог IMO та WCO. Для прискорення розроблення стандарт ISO 28005 було поділено на дві частини:

Стандарт ISO 28005-1 «*Повідомлення структур*»;

Стандарт ISO/FAS 28005-2:2009 *«Елементи основних даних»*.

Стандарт ISO 28006 *«Управління безпекою RO-RO пасажирських поромів. Найкраща практика застосування заходів безпеки»*.

Стандарт ISO 20858:2007 *«Судна і морські технології. Оцінювання безпеки споруд морських портів і розроблення планів безпеки»* забезпечує застосування Кодексу безпеки портів.

Діяльність з кібер-безпеки. Рішення для бізнесу

Едвард Хемфрі[6]

Існує багато різноманітних історій про кібер-загрози, з якими стикаються підприємства, уряди та громадяни. Це не просто чутки, такі загрози є реальними, а їхній вплив є досить значним.

Питання кібер-безпеки постало задовго до загальновідомого скандалу з WikiLeaks. Відомо багато повідомлень щодо випадків крадіжки особистої інформації та даних стосовно клієнтів, у тому числі сотні тисяч номерів соціального страхування. Інші кібер-загрози охоплюють поширені крадіжки особистих даних, інтернет-шахрайства та злочини проти дітей.

Однією з найтривожніших подій 2010 року стала поява комп'ютерного «хробака Stuxnet», який став загрозою для безпеки промислових систем, таких як АЕС-контролери, гідроелектростанції, електричні мережі та інші енергетичні об'єкти. Частота і складність цього виду шкідливих програм, а також питання стосовно можливої мотивації злочинців викликають стурбованість урядів та інших схильних до ризику інфраструктур.

«Хробак Stuxnet» виявив уразливі місця Інтернет-комунікацій, а також той факт, що деякі частини національної інфраструктури можна розглядати як «бомбу сповільненої дії». Але це не єдина галузь, що є вразливою для кібер-війни в багатьох країнах.

[6] Професор Едвард Хамфрі протягом 35 років працював у сфері інформаційної безпеки у великих міжнародних компаніях Європи, Північної Америки та Азії, а також у таких організаціях та установах, як Європейська Комісія, Рада Європи та Організація економічного співробітництва та розвитку (OECD). Він є керівником робочої групи ISO/IEC з питань розроблення стандартів на ISMS. Професор Едвард Хамфрі читає лекції в університетах по всьому світові і видав декілька видатних книг з питань упровадження стандартів ISMS.

Стандарти на кібер-безпеку

Чи можливо, що web-середовище, яке використовують бізнес, уряди та громадяни, у майбутньому буде безпечним? Чи повністю усвідомлюють компанії та уряди ризики й наслідки, з якими вони стикаються?

Загальна відповідь полягає в тому, що більшість організацій все ще не вжили відповідних заходів з приводу урахування ризиків безпеки та захисту себе і своїх активів від них. Ці заходи охоплюють оцінення ризиків, упровадження засобів контролю безпеки з метою зменшення цих ризиків, регулярний моніторинг та аналіз ефективності елементів управління, переоцінення ризиків і внесення необхідних змін, якщо рівень ризику зростає.

Іншими словами, підхід до ризику — це постійне вдосконалення процесів, які мають проводити організації, поки не будуть повністю захищені.

Стандарт ISO/IEC 27001:2005 *«Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги»* було прийнято сотнями тисяч організацій для упровадження відповідних процесів управління ризиками. Стандарт ISO/IEC 27001 забезпечує ефективну структуру управління інформаційною безпекою, оскільки враховує усі потреби та бізнес-вимоги організації у галузі безпеки і здатен розвиватися з метою підвищення рівня захисту відповідно до зміни кібер-загрози.

Багато програм, розроблюваних для захисту від кібер-загроз, розробляють з посиланням на стандарти ISO/IEC 27001 та ISO/IEC 27002:2005 *«Інформаційні технології. Методи убезпечення. Кодекс практики з управління інформаційною безпекою»*. Одним з таких заходів є програма Національної безпеки США, яка посилається на ці стандарти як основу для створення надійної системи управління інформаційною безпекою.

Стандарт ISO/IEC 27001 встановлює ряд настанов, на яких засновано всі стандарти так званої серії стандартів на системи управління інформаційною безпекою (ISMS), стандарти ISO/IEC серії 27000, до якої належать:

- стандарт ISO/IEC 27002:2005 *«Інформаційні технології. Методи убезпечення. Кодекс практики з управління інформаційною безпекою»;*
- стандарт ISO/IEC 27003:2010 *«Інформаційні технології. Методи убезпечення. Настанови з упровадження системи управління інформаційною безпекою»;*
- стандарт ISO/IEC 27004:2009 *«Інформаційні технології. Методи убезпечення. Управління інформаційною безпекою. Вимірювання»;*
- стандарт ISO/IEC 27005:2011 *«Інформаційні технології. Методи убезпечення. Управління ризиками інформаційної безпеки»*.

Ще однією важливою особливістю стандарту ISO/IEC 27001 є те, що він може бути використаний для сертифікації, тобто організація забезпечить належне оцінення своєї ISMS. Це надає впевненість і забезпечує те, що ISMS організації «придатні для досягнення успіху». Понад 12 000 організацій було сертифіковано на відповідність вимогам ISO/IEC 27001 з того часу, як стандарт було уперше опублікований ISO. Кількість підприємств, які пройшли сертифікацію на відповідність вимогам стандарту ISO/IEC 27001, щороку зростає втричі, що демонструє користь стандарту для вирішення проблем ризиків організації.

Приборкання «кібер-тигра»

Ще одна сфера, на якій зосереджено увагу ISO, це інциденти з інформаційної безпеки. Організаціям важливо мати інформацію про кібер-інциденти, щоб ефективно на них реагувати та належним чином обмежувати їхній вплив.

Час має суттєве значення, оскільки, що більше часу витрачається на контроль та ліквідацію наслідків інциденту, то більша ймовірність того, що їхній вплив буде проникати глибше в систему організації. Якщо інцидент ламає бізнес-систему, то організація не може нормально працювати. Питання полягає лише в тому, як довго організація може миритися з перебуванням своєї системи в автономному режимі.

Як довго клієнти можуть чекати доступу до мережі Інтернет: від 24 до 48 годин? Чи можливо межа — це 12 години або ще менше? Як довго існуватиме компанія, якщо вона не здатна надавати послуги, і скільки це будуть терпіти клієнти, перш ніж почнуть змінювати постачальників? Ці питання особливо важливі для фінансової системи, он-лайн бронювання, постачання електроенергії та управління газопостачанням та інших систем, що забезпечують обслуговування клієнтів.

Інформаційні та комунікаційні технології (ІСТ) стали невід'ємною частиною важливих інфраструктур усіх сфер, будь-то державні, приватні або благодійні. Поширення мережевих послуг та розширення можливостей систем та програм означає, що організації все більше залежать від безпечної та надійної інфраструктури ІСТ. Порушення роботи цих систем, у тому числі через такі загрози для безпеки, як злом і шкідливі програми, негативно впливають на безперервність бізнес-операцій.

Діяльність організації, яка вимагає безперервних процесів, як правило, залежить від ІСТ. Це означає, що порушення ІТС може завдати шкоди репутації підприємства. Під час підготовки підприємства до безперервного ведення бізнесу використовують стандарт ISO/IEC 27031:2011 *«Інформаційні технології Методи убезпечення. Настанови щодо*

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.