Стаття публікується у [Інформаційному бюлетені з міжнародної стандартизації 3-2011]

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.

Новина щодо інформаційної діяльності сайту WikiLeaks поширилася подібно лісовій пожежі через світову пресу, телебачення та Internet-форуми. Результатом такої уваги стало те, що хакери активізували кібер-війну, встановлюючи на свої комп'ютери програмне забезпечення, яке дозволяє стати учасником запуску атак проти комерційних компаній.

Вважається, що в руках WikiLeaks знаходяться 260 000 секретних документів з Державного департаменту США, а викладено було менше одного відсотка від цього скарбу. WikiLeaks опублікувала секретну інформацію, яка потенційно становить небезпеку для життя американців та інфраструктури країни, а також впливає на національну безпеку. Діяльність WikiLeaks також вплинула на багато комерційних Internet-компаній.

Однією з груп, що бере участь у кібер-війні, є тіньова організація хакерів під назвою "Операція розплата" (Operation Payback), яка здійснила координацію ряду успішних розподілених атак типу "відмова в обслуговуванні" (DDoS) атак на PayPal, Visa, MasterCard і Amazon. Хоча "Операція розплата" не має ніяких очевидних зв'язків з WikiLeaks та обидві ці групи мають аналогічні цілі, вимагають прозорості та скасування цензури. Все це може бути визначено, як перша реальна інформаційна війна.

Питання кібер-безпеки постало задовго до загальновідомого скандалу з WikiLeaks. Відомо багато повідомлень про випадки крадіжки особистої інформації і даних про

клієнтів, у тому числі, сотні тисяч номерів соціального страхування. Інші кібер-загрози охоплюють поширені крадіжки особистих даних, Internet-шахрайства та злочини проти дітей.

Однією з найбільш тривожних 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 про можливу мотивацію злочинців викликають стурбованість урядів та інших схильних до ризику інфраструктур.

"Хробак Stuxnet" виявив вразливі місця Internet-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.

Зараз, ймовірно, відбувається лише увертюра до "вистави". Якщо загроза відбудеться, наслідки можуть бути катастрофічними для урядів, комерційних організацій та приватних осіб.

Стандарти на кібер-безпеку

Чи можливо, що web-середовище, яке використовується бізнесом, урядами та громадянами, у майбутньому буде безпечним? Чи повністю усвідомлюють компанії і уряди ризики та наслідки, з якими вони стикаються?

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

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

Стандарт ISO/IEC 27001:2005 “Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпеки. Вимоги” був прийнятий сотнями тисяч організацій для впровадження 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, що розробляються для захисту від кібер-загроз розробляються з посиланням на стандарти ISO/IEC 27001 та ISO/IEC 27002:2005 “Інформаційні технології. Методи забезпечення безпеки. 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 засновані 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 забезпечення безпеки. Кодекс практики з управління інформаційною безпекою”;

-

стандарт ISO/IEC 27003:2010 “Інформаційні технології. Методи забезпечення безпеки. Настанови з впровадження системи управління інформаційною безпекою”;

-

стандарт ISO/IEC 27004:2009 “Інформаційні технології. Методи забезпечення безпеки. Управління інформаційною безпекою. Вимірювання”;

-

стандарт ISO/IEC 27005:2011 “Інформаційні технології. Методи забезпечення безпеки.

Управління ризиками інформаційної безпеки".

Ще однією важливою особливістю стандарту ISO/IEC 27001 є те, що він може бути використаний для сертифікації, тобто організація забезпечить належну оцінку своєї ISMS. Це надає впевненість і забезпечують те, що ISMS організації "придатні для досягнення успіху". Більше 12000 організацій були сертифіковані на відповідність вимогам ISO/IEC 27001 з того часу, як стандарт був вперше опублікований ISO п'ять років тому. Кількість підприємств, що пройшли сертифікацію на відповідність вимогам стандарту ISO/IEC 27001, кожного року зростає втричі, що відображає користь стандарту для вирішення проблем ризиків організації.

Приборкання кібер-тигра

Ще одна сфера, на якій зосереджена увага 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 чим більше часу витрачається на контроль та ліквідацію наслідків інциденту, тим більша ймовірність того, що їхній вплив буде проникати глибше в систему організації. Якщо інцидент ламає бізнес-систему, то організація не може вести нормальну роботу (малюнок 1). Питання полягає тільки в тому, як довго організація може миритися з перебуванням своєї системи в автономному режимі.

Як довго клієнти можуть чекати доступу до Internet: 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 (ICT) стали невід'ємною частиною важливих

інфраструктур всіх сфер, будь-то державні, приватні або благодійні. Поширення мережевих послуг та розширення можливостей систем та програм також означає, що організації все більше залежать від безпечної та надійної інфраструктури ІСТ. Порушення роботи цих систем, в 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 використовується стандарт ISO/IEC 27031:2011 “Інформаційні технології. Методи забезпечення безпеки. 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 виконувати копіювання в 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 в 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 з стандартами ISO/IEC серії 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 повинні 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.

Історія з WikiLeaks є сенсаційною новиною сьогоднішнього дня, але вона може бути легко затьмарена іншою кібер-воєнною історією завтра. Організації не повинні піддаватися спокусі та заспокоювати себе думкою "це не станеться з нами". Ризики існують завжди через те, що організації використовують однакові технології та програми, спілкуються через мережу Internet, отже, бути підготовленим — це просто здоровий глузд.

Едвард Хемфрі, ISO Focus +