УДК 004.056.5

Стародубець О.В., студент групи 125м-16-1,
Науковий керівник: Тимофєєв Д. С., ст. викл. кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

ВПРОВАДЖЕННЯ СИСТЕМ МОНІТОРИНГУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

В наш час серйозно ускладнюється інфраструктури організацій всіх можливих галузей, від банків і до державних організацій. В першу чергу це пов'язано з швидким розвитком технологій і різновидів електронних пристроїв які оброблюють інформацію, тому така тенденція формує потребу в захисті та автоматизації інформаційних активів.

На даний момент підхід до контролю потенційно небезпечних подій у вигляді декількох незалежних засобів захисту інформації з самостійними консолями, які як правило контролюються різними людьми, стає надмірно ресурсномістким і неефективним, в результаті чого адекватна і своєчасна реакція на них стає все більш трудомісткою. Складність забезпечення відповідної реакції на потенційно небезпечні події неминуче призводить до зниження ефективності системи інформаційної безпеки організації. Рішенням такого завдання є створення центру моніторингу і реагування, який будується на регламентах, процесах, кваліфікованих кадрах і грамотному технічному рішенні.

Компанії, впроваджуючи основні елементи безпеки, часто не приділяють належної уваги такому важливому елементу забезпечення інформаційної безпеки, як моніторинг системи інформаційної безпеки.

В результаті, витративши сили і засоби на впровадження засобів захисту, компанії вважають завдання виконаним, але на перевірці виявляється, що:

- критичні системи уразливі і доступні для зловмисників;
- на робочих станціях встановлено недозволене ПО;
- конфігурації не відповідають розробленим політикам;
- події, які свідчать про інцидент ІБ, залишаються непоміченими;
- виявивши інцидент ІБ, немає чітко визначеної процедури, що з ним робити далі і хто цим повинен займатися;
- у адміністраторів інформаційної безпеки немає повної і цілісної картини про стан ІБ, є тільки фрагментарні уявлення;
- і т.д.

Комплексний моніторинг ІБ передбачає збір та аналіз подій безпеки від різних систем захисту, пристроїв і додатків, збір конфігураційних даних, даних про уразливість і т.д. Це дозволяє отримати повну і достовірну інформацію про наявні події і вразливості ІБ, поточних налаштуваннях, тобто мати цілісну картину поточної захищеності компанії. Здійснюючи такий контроль, організації мають можливість оперативного управління інформаційною безпекою, виявляючи відхилення, своєчасно вирішуючи інциденти ІБ, усуваючи уразливості, вживаючи заходів щодо корегування засобів захисту і т.д.

Підтвердження важливості і необхідності комплексного моніторингу знайшло відображення в різних стандартах в області інформаційної безпеки, таких, як: PCI DSS, ISO / IEC 27001: 2013, SOX.

Прикладом системи комплексного моніторингу ІБ на підприємстві є SOC.

SOC – Security Operations Center, або Центр оперативного управління, основними завданнями якого є консолідація подій з багатьох джерел, проведення певної аналітики і оповіщення уповноважених співробітників про інциденти інформаційної безпеки чи інших подіях. На основі отриманих даних співробітники центру проводять

розслідування, вживають заходів, щоб виключити можливість повторення події, мінімізують втрати. [1]

Ситуаційний центр являє собою комплексне організаційно-технічне рішення, що дозволяє:

• автоматизовано виявляти події, що представляють потенційну загрозу для організації, її інформаційних систем або інформаційних активів;

• забезпечити тривале зберігання всього обсягу зібраних подій і зафіксованих інцидентів ІБ для можливості проведення постінцідентного розслідування;

• реалізувати процес обробки виявлених інцидентів, який би дозволив в гарантований час (залежне від рівня критичності інциденту) оповіщати відповідальні підрозділи організації про те, що сталося, і рекомендувати необхідні заходи для запобігання впливу інциденту інформаційної безпеки на бізнес.

Зібрана в ході комплексного моніторингу інформація надходить в єдиний центр, де вона обробляється і представляється в наочному і зручному вигляді. Тут же здійснюється реагування та вирішення інцидентів ІБ, усунення виявлених відхилень. Побудова такого Центру оперативного управління ІБ (Security Operations Center, SOC) є не простим завданням.

Центр оперативного управління ІБ дозволяє контролювати і оперативно управляти інформаційною безпекою компанії в режимі реального часу, бути впевненим в тому, що необхідний рівень забезпечення ІБ досягнутий і підтримується, відстежувати виконання заданих цільових показників ефективності (KPI) забезпечення ІБ.

Центр оперативного управління ІБ дозволяє відстежувати відповідні в інформаційній системі події, пов’язані з ІБ, аналізувати і зіставляти їх з іншими даними, представляти зібрану інформацію в наочному і зручному вигляді, контролювати наявні уразливості, здійснювати контроль конфігурацій, відстежувати ступінь виконання вимог законодавства, нормативних актів і корпоративних політик, а також оперативно реагувати на виявлені інциденти ІБ. Тобто представлять повну картину поточного стану інформаційної безпеки компанії, що дозволяє оперативно усувати виявлені відхилення і забезпечувати заданий рівень ІБ.

На завершення необхідно відзначити основні переваги, які дає створення SOC ІБ, - це швидкість реакції на інциденти і підвищення керованості процесу забезпечення ІБ.

Час протікання більшості інцидентів у сфері інформаційної безпеки становить не більше секунди, а наслідки цих секундних збоїв можуть бути катастрофічні. У свою чергу, побудова SOC ІБ, за даними західних досліджень, знижує затримки реагування на інциденти ІБ через людський фактор на 80-90%.

Другим важливим перевагою є можливість бачити зріз стану інформаційної безпеки в комплексі, в режимі реального часу.

Можна виділити і більш приватні переваги, такі як:

• зниження ризиків і часу простою в критичних бізнес-процесах;

• контроль і запобігання інцидентів безпеки. Скорочення термінів робіт з розслідування інцидентів та надання звітів керівництву;

• вивільнення ресурсів фахівців інформаційної безпеки та IT-служби, оскільки вони витрачають багато часу на консолідацію і аналіз інцидентів, пов’язаних з порушеннями політики інформаційної безпеки компанії;

• відповідальність за процес;

• розстановка пріоритетів по ризиках для прийняття адекватних заходів захисту.

ПЕРЕЛІК ПОСИЛАНЬ

1. Єршов В.О. SOC vs CERT: Подібність і відмінності (Електрон. ресурс) / Спосіб доступу: URL: https://www.anti-malware.ru/node/16464