© Kinzeryavyy V., Gnatyuk V. Basic performance parameters for cyberincidents response teams // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 2, p. 193-196.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ / INFORMATION SECURITY MANAGEMENT

БАЗОВІ ПОКАЗНИКИ ЕФЕКТИВНОСТІ РОБОТИ КОМАНД РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

Василь Кінзерявий, Віктор Гнатюк

Національний авіаційний університет, Україна

КІНЗЕРЯВИЙ Василь Миколайович, к.т.н.

Рік та місце народження: 1985 рік, м. Кам'янець-Подільський, Хмельницька область, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: доцент кафедри безпеки інформаційних технологій з 2014 року.
Наукові інтереси: інформаційна безпека, криптографія та криптоаналіз блокових симетричних шифрів.
Публікації: більше 50 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях, авторські свідоцтва.
E-mail: 0werl0rd@ukr.net

ГНАТЮК Віктор Олександрович

Рік та місце народження: 1990 рік, м. Нетішин, Хмельницька область, Україна.
Освіта: Хмельницький національний університет, 2012 рік.
Посада: аспірант кафедри безпеки інформаційних технологій з 2012 року.
Наукові інтереси: інформаційна безпека, управління інцидентами інформаційної безпеки.
Публікації: більше 20 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях, авторські свідоцтва.
E-mail: viktorgnatyuk@meta.ua

Анотація. *Основними етапами управління інцидентами інформаційної безпеки є реагування та розслідування – ці функції покладені на спеціалізовані команди і центри (типу CERT – Computer Emergency Response Team). Від ефективності роботи останніх залежить рівень інформаційної безпеки як окремої організації, так і держави в цілому. Проведений аналіз показав, що оцінювання продуктивності роботи CERT не проводиться належним чином, тому у цій статті було введено базові показники ефективності роботи команд реагування на кіберінциденти – це дало можливість оцінювати ефективність роботи CERT за необхідний період. Звіт за такими показниками варто проводити регулярно, наприклад, раз на тиждень (місяць, рік і т.п.), щоб отримати повну картину їх змін та визначити основні тенденції. Використання отриманих показників дасть можливість: швидко приймати управлінські рішення, оцінювати рівень кваліфікації фахівців CERT, підвищити ефективність роботи CERT, зменшити втрати пов'язані з інцидентами, підвищити продуктивність роботи користувачів, ефективно використовувати персонал тощо. Крім того, шляхом впливу на дії фахівців CERT та їх корегуванням, можна підвищити рівень інформаційної безпеки окремої організації та держави в цілому. У подальшому, на основі цих показників, планується побудувати математичні моделі з метою забезпечення безперервного поліпшення ефективності процесу управління кіберінцидентами.*

Ключові слова: *інцидент, управління інцидентами, кіберінцидент, інформаційна безпека, CERT, команда реагування на кіберінциденти, показники ефективності.*

Вступ. Одним із важливих етапів менеджменту інформаційної безпеки (ІБ) є управління інцидентами [1]. Відповідно до [2] існує багато підходів до визначення поняття «інцидент», його класифікації та відокремлення від інших суміжних понять (наприклад, подія безпеки, інцидент безпеки, кіберінцидент тощо). Функції реагування на інциденти та їх розслідування покладаються на відповідні спеціалізовані команди та центри (типу CERT – Computer Emergency Response Team). Відповідно до [3] сфера діяльності CERT включає, серед іншого, заходи, спрямовані на ліквідацію інцидентів ІБ, які виникають в інформаційному (кібер) просторі. Сьогодні у світі

функціонують команди реагування на кіберінциденти (CERT). Згідно [3] їх налічується 284 з 61 країни світу. Як показав проведений аналіз, оцінці ефективності роботи CERT не приділяється достатньо уваги, а оскільки, від продуктивності роботи цих команд залежить ІБ як окремої організації, так і держави в цілому. З огляду на це, оцінювання роботи CERT є надзвичайно **актуальним** науково-технічним завданням.

Метою даної роботи є введення базових показників ефективності роботи команд реагування на кіберінциденти.

Основна частина

Відомо, що бібліотека інфраструктури інформаційних технологій (ITIL) використовує широке визначення терміну «інцидент», тому майже всі звернення користувачів можуть реєструватися і відслідковуватися як інциденти. У книзі «Підтримка послуг» [6] бібліотеки ITIL дається таке визначення: інцидент - це будь-яка подія, яка не є частиною стандартних операцій з надання послуги, що призвела або може призвести до порушення або зниження якості цієї послуги. У контексті бібліотеки ITIL інцидентами вважаються не тільки помилки в роботі (використанні) апаратного або програмного забезпечення, але також і запити на обслуговування. Запит на обслуговування - це запит від користувача на підтримку, надання інформації, консультації або документації, який не є збоєм ІТ-інфраструктури.

З огляду на роботи [4,5], кожне звернення до CERT – Z_j, де j - порядковий номер звернення, повинно описуватись множиною параметрів:

$$Z_j \in \left\{ІЗ^j, Т_{від}^{\ j}, Т_{зак}^{\ j}, К_{поч}^{\ j}, К_{кін}^{\ j}, П_п^{\ j}, Р_{кін}^{\ j}, С_{звер}^{\ j}, ТР_n^{\ j}, ТВ_n^{\ j}, К_{некор}^{\ j}, О_{клієн}^{\ j}, І_{проак}^{\ j}, В_{зах}^{\ j}, Т_{ріш}^{\ j}\right\}.$$

Параметри звернень Таблиця 1

Параметр	Опис	Можливі значення
ІЗ	інцидент або запит на надання послуг	1-інцидент, 0-запит
$Т_{від}$	відкриття	час, дата
$Т_{зак}$	закриття	час, дата
$К_{поч}$	початкова категорія	1,2,3…n - категорія
$К_{кін}$	кінцева категорія	1,2,3…n - категорія
$П_п$	пріоритет	1,2,3…n - пріоритет
$Р_{кін}$	кінцевий рівень вирішення	1,2,3,4 - рівні
$С_{звер}$	стан	0-відкрите, 1-закрите
$ТР_n$	тривалість розгляду на n -му рівні	час, дата
$ТВ_n$	тривалість вирішення на n -му рівні	час, дата
$К_{некор}$	некоректні призначення	од.
$О_{клієн}$	оцінка клієнта	0,1,2,3,4,5
$І_{проак}$	вирішення проактивне	1-так, 0-ні
$В_{зах}$	вартість заходів реагування	у.о.
$Т_{ріш}$	відведений час на рішення відповідно до пріоритету	час, дата

У табл. 1 показано параметри звернень, що надходять до CERT, їх опис та можливі значення.

Запропоновано показники за допомогою яких можна оцінювати ефективність роботи CERT за необхідний період:

1) загальна кількість звернень:

$$К_{зверн} = TS+TN,$$

де TS - загальна кількість запитів на надання послуг:

$$TS = \sum_{j=1}^{К_{зверн}} 1, \forall Z_j, \text{ для якого } ІЗ^j = 0,$$

TN - загальна кількість інцидентів:

$$TN = \sum_{j=1}^{К_{зверн}} 1, \forall Z_j, \text{ для якого } ІЗ^j = 1;$$

2) загальна кількість закритих інцидентів:

$$TN_{end} = \sum_{i=1}^{К_{зверн}} 1, \forall Z_j, \text{ для якого } С_{звер}^j = 1, ІЗ^j = 1.$$

Наведемо приклад. Нехай маємо 5 інцидентів, 3 з яких закриті, відповідно $TN_{end} = 3$;

3) інциденти вирішені на n -му рівні підтримки:

$$Q_{fln} = \sum_{j=1}^{К_{звери}} 1, \forall Z_j, \text{ для якого } С_{звер}^j = 1, Р_{кін}^j = n \text{ рівень}, ІЗ^j = 1.$$

Припустимо є 3 закриті інциденти. Рівень вирішення 1-го інциденту «3», 2-го інциденту «2», 3-го інциденту «2». Звідси, $Q_{fl2} = 2$ од;

4) середня тривалість обробки інциденту на n -му рівні:

$$Т_{серп} = \frac{\sum_{j=1}^{TN} ТР_n^j, ІЗ^j = 1}{TN_n},$$

де TN_n - загальна кількість інцидентів на n-му рівні.

Перед тим,як співробітник CERT займеться вирішенням інциденту, або ж його передачею на наступний рівень підтримки проходить певний час розгляду інциденту. Припустимо, що є 3 інциденти. Час розгляду 1-го інциденту на 2-му рівні підтримки складає 123 с., 2-го інциденту – 54 с., 3-го інциденту – 362 с. Отже, $Т_{сере2} = \frac{123+54+362}{3} = 179,66$ с;

5) кількість інцидентів некоректно призначених на співробітників CERT:

$$Q_{pds} = \sum_{j=1}^{K_{зверн}} 1, \forall Z_j, \text{ для якого } K^j_{некор} > 0, ІЗ^j = 1.$$

Нехай маємо 3 інциденти, 2 з яких некоректно призначені співробітникам CERT, відповідно: $Q_{pds} = 2$ од ;

6) кількість закритих інцидентів некоректно призначених на співробітників CERT:

$$Q_{pdsend} = \sum_{j=1}^{K_{зверн}} 1, \forall Z_j, \text{ для якого } K^j_{некор} > 0, C^j_{звер} = 1, ІЗ^j = 1.$$

Розраховується аналогічно попередньому показникові, єдина умова, інцидент має бути закритим;

7) інциденти, вирішені протягом заданого часу відповідно до пріоритету:

$$Q_{ap} = \sum_{j=1}^{K_{зверн}} 1, \forall Z_j, \text{ для якого } C^j_{звер} = 1, (T^j_{зак} - T^j_{від}) \le T^j_{ріш}, ІЗ^j = 1.$$

Припустимо, що є 3 закриті інциденти з пріоритетом «2». Кожен інцидент, згідно пріоритету, має відведений час рішення. Час відкриття 1-го інциденту – 11:12:30 дата 17.05.14, час закриття – 12:40:36 дата 17.05.14; час відкриття 2-го інциденту – 12:12:52 дата 17.05.14, час закриття – 14:10:14 дата 17.05.14; час відкриття 3-го інциденту – 20:50:34 дата 17.05.14, час закриття – 01:40:43 дата 18.05.14. Час відведений на рішення інциденту відповідно пріоритету «2» складає 2 год.=7200 с. Для зручності, його переведено у секунди та обчислено час затрачений на вирішення інцидентів. 1-й інцидент – 5286 с., 2-й інцидент – 7042 с., 3-й інцидент – 17408 с. Звідси, $Q_{ap} = 2$ од ;

8) середній час вирішення інциденту на n -му рівні підтримки:

$$T_{cpsn} = \frac{\sum_{j=1}^{TN} TB^j_n, ІЗ^j = 1}{TN_n}.$$

Нехай, на 1-му рівні підтримки вирішено 3 інциденти. Тривалість вирішення першого складає 4625 с., другого – 7569 с., третього – 5563 с. Звідси $T_{cps1} = \frac{4625+7569+5563}{3} = 5919$ с;

9) середня тривалість вирішення інциденту:

$$T_{срв} = \frac{\sum_{j=1}^{K_{зверн}} (T^j_{зак} - T^j_{від}), \forall Z_j, \text{ для якого } C^j_{звер} = 1, ІЗ^j = 1}{TN_{end}}.$$

Припустимо, є 3 закриті інциденти, тривалість вирішення першого складає 3625 с., другого – 8569 с., третього – 4563 с. Звідси $T_{срв} = \frac{3625+8569+4563}{3} = 5585,66$ с;

10) неправильно класифіковані інциденти:

$$Q_{is} = \sum_{j=1}^{K_{зверн}} 1, \forall Z_j, \text{ для якого } C^j_{звер} = 1, K^j_{поч} \ne K^j_{кін}, ІЗ^j = 1.$$

При реєстрації кожного звернення призначається категорія, що полегшує його обробку і подальший аналіз. Коли звернення закривається, у відповідному записі вказується його справжня категорія. Показник відображає, скільки разів дві категорії не співпали. Припустимо, що є 5 закритих інцидентів початкова категорія інциденту не відповідає кінцевій у 3-х з них. Відповідно $Q_{is} = 3$ од;

11) звернення, що надійшли до фахівців CERT «напряму», минаючи 1-й рівень:

$$Q_{pfl} = \sum_{j=1}^{K_{зверн}} 1, \forall Z_j, \text{ для якого } (TP^j_1 + TB^j_1) = 0.$$

На кожне звернення відводиться час для його розгляду та вирішення. Даний показник фіксує всі звернення, на які не було витрачено часу на 1-му рівні. Припустимо, що маємо 100 звернень. Час затрачений на розгляд та вирішення на 1-му рівні відсутній у 5 зверненнях. Відповідно $Q_{pfl} = 5$ од;

12) середня оцінка задоволеності клієнтів:

$$CS = \frac{\sum_{j=1}^{K_{зверн}} O^j_{клієн}}{K_{зверн}}.$$

Якщо звернення «закриваються» дуже швидко або обслуговуються занадто довго, то незалежно від того, що відображають інші показники, оцінка задоволеності клієнтів почне знижуватися і даний показник це відобразить. Припустимо, що CERT опрацював 5 звернень, клієнти виставили за 5-ти бальною шкалою (від 0 до 5) відповідні оцінки: 1-е звернення «5», 2-е звернення «4», 3-е звернення «5», 4-е звернення «2», 5-е звернення «0». Розрахуємо $CS = \frac{5+4+5+2+0}{5} = 3,2$;

13) загальна кількість інцидентів правильно вирішених з першого разу:

$$Q_{rsf} = TN_{end} - Q_{pdsend}.$$

Нехай маємо загальну кількість закритих інцидентів, яка складає 100 од., і маємо загальну кількість інцидентів некоректно призначених на співробітників служби підтримки – 90 од., тоді $Q_{rsf} = 100 - 90 = 10$ од;

14) загальна кількість інцидентів вирішених проактивно:

$$Q_{гр} = \sum_{j=1}^{K_{зверн}} 1, \forall Z_j, \text{ для якого } C^j_{звер} = 1, I^j_{проак}, ІЗ^j = 1.$$

Даний показник розраховується додаванням закритих інцидентів, які були вирішені проактивно. Припустимо, що є 100 закритих інцидентів, з них вирішено проактивно – 5 од. Отже, $Q_{гр} = 5$;

15) середній час вирішення інцидентів за пріоритетами:

$$T_{cpNi} = \frac{\sum_{j=1}^{K_{зверн}} (T^j_{зак} - T^j_{від}), \forall Z_j, \text{ для якого } C^j_{звер} = 1, П^i_n = i}{TN_{endi}},$$

де TN_{endi} - загальна кількість закритих інцидентів за і-м пріоритетом.

Припустимо, що за пріоритетом «1» маємо 3 закриті інциденти: час відкриття 1-го інциденту – 11:12:30 дата 17.05.14, час закриття – 12:40:36 дата 17.05.14; час відкриття 2-го інциденту – 12:12:52 дата 17.05.14, час закриття – 14:10:14 дата 17.05.14; час відкриття 3-го інциденту – 20:50:34 дата 17.05.14, час закриття – 01:40:43 дата 18.05.14. Для зручності переведемо у секунди і порахуємо час затрачений на вирішення інцидентів. 1-й інцидент – 5286 с., 2-й

інцидент – 7042 с., 3-й інцидент – 17408 с. Тепер розрахуємо $T_{cpN1} = \frac{5286 + 7042 + 17408}{3} = 9912$ с.=2 год 45 хв 12 с;

16) середня вартість заходів реагування на інцидент:

$$ACR = \frac{\sum_{j=1}^{K_{звери}} B^j_{зах}, \forall Z_j, \text{для якого } I3^j = 1, C^j_{звер} = 1}{TN_{end}}.$$

Наприклад, візьмемо 3 закриті інциденти, вартість заходів реагування на 1-й інцидент складає 100 у.о., 2-й – 150 у.о., 3-й – 250 у.о. Звідси, $ACR = \frac{100 + 150 + 250}{3} = 166,66$ у.о.

Висновки

Таким чином, було введено базові показники ефективності роботи груп реагування на кіберінциденти. Звіт за такими показниками варто проводити регулярно, наприклад раз на тиждень (місяць, рік і т.п.), щоб отримати повну картину їх змін та визначити основні тенденції. Використання отриманих показників дасть можливість: швидко приймати управлінські рішення, оцінювати рівень кваліфікації фахівців CERT, підвищити ефективність роботи CERT, зменшити втрати пов'язані з інцидентами, підвищити продуктивність роботи користувачів, ефективно використовувати персонал, підвищити точність інформації в конфігураційний базі даних (CMDB), підвищити задоволеність користувачів і замовників тощо. Крім того, шляхом впливу на дії фахівців CERT та їх корегуванням, можна підвищити рівень ІБ окремої організації та держави в цілому.

У подальшому, на основі цих показників, планується побудувати математичні моделі з метою забезпечення безперервного поліпшення ефективності процесу управління кіберінцидентами.

Література

[1] ISO / IEC 27035:2011, Information technology – Security techniques – Information security incident management. — 2011. — 78 p.

[2] Гнатюк В.О. Аналіз дефініцій поняття «інцидент» та його інтерпретація у кіберпросторі // В.О. Гнатюк / Безпека інформації. – №3 (19). – 2013. – С. 175-180.

[3] Computer Emergency Response Team of Ukraine [Електронний ресурс]. - Режим доступу: http://cert.gov.ua/?page_id=207. (04.06.14)

[4] Бон Я.В. ИТ Сервис-менеджмент, введение / под ред. Яна Ван Бона; пер. с англ. осуществлен компанией «IT Expert», 2003. – 240 с.

[5] Брукс П. Метрики для управления ИТ-услугами / П. Брукс; пер. с англ. – М.: Альпина Бизнес Букс, 2008. – 283 с.

[6] ITIL. Поддержка услуг. — М.: Ай-Теко, 2009. — 418 с.

УДК 004.056.5 (045)

Кинзерявый В.Н., Гнатюк В.А. Базовые показатели эффективности работы команд реагирования на киберинциденты

Аннотация. *Основными этапами управления инцидентами информационной безопасности является реагирование и расследование - эти функции возложены на специализированные команды и центры (типа CERT – Computer Emergency Response Team). От эффективности работы последних зависит уровень информационной безопасности, как отдельной организации, так и государства в целом. Проведенный анализ показал, что оценка производительности работы CERT не проводится должным образом, поэтому в этой статье было введено базовые показатели эффективности работы команд реагирования на киберинциденты - это дало возможность оценивать эффективность работы CERT за необходимый период. Отчет по таким показателям следует проводить регулярно, например, раз в неделю (месяц, год и т.п.), чтобы получить полную картину их изменений и определить основные тенденции. Использование полученных показателей позволит: быстро принимать управленческие решения, оценивать уровень квалификации специалистов CERT, повысить эффективность работы CERT, уменьшить потери связанные с инцидентами, повысить производительность работы пользователей, эффективно использовать персонал и т.д.. Кроме того, путем влияния на действия специалистов CERT и их корректировкой, можно повысить уровень информационной безопасности отдельной организации и государства в целом. В дальнейшем, на основе этих показателей, планируется построить математические модели с целью обеспечения непрерывного улучшения эффективности процесса управления киберинцидентами.*

Ключевые слова: *инцидент, управления инцидентами, киберинцидент, информационная безопасность, CERT, команда реагирования на киберинциденты, показатели эффективности.*

Kinzeryavyy V., Gnatyuk V. Basic performance parameters for cyberincidents response teams

Abstract. *The main stages of information security incidents management are responding and investigation. These functions are assigned to specialized teams and centers (such as CERT – Computer Emergency Response Team). The information security level of organization and whole state depends on CERT`s performance. The analysis showed that CERT`s performance assessment is not carried out properly. That's why in this paper basic performance parameters for cyberincidents response teams – it gives a possibility to assess CERT`s performance during necessary period. The report on these parameters should be performed regularly such as once a week (month, year etc.) to obtain a complete picture of their changes and identify key trends. Using the obtained parameters will enable: to make quick management decisions, evaluate the level of CERT`s specialists, to improve the CERT efficiency, to reduce losses associated with incidents, to improve user productivity, to use staff effectively and others. As well by influencing on the CERT`s specialists actions and their correction can improve information security level of organization and whole state. Further on the basis of these parameters it is planned to develop mathematical models to ensure continuous improvement of the cyberincidents management.*

Key words*: incident, incident management, cyberincident, information security, CERT, cyberincidents response teams, performance parameters.*

Отримано 4 *червня 2014 року*, затверджено редколегією 27 *червня 2014 року*