СПОСОБ ОПРЕДЕЛЕНИЯ РЕГИСТРИРУЕМЫХ СОБЫТИЙ

Кузнецов А.В.[1], Ненашев С.М.[2]

В статье источник событий, осуществляющий непосредственную регистрацию событий, рассмотрен как основа для инфраструктуры управления событиями в составе системы управления информационной безопасностью предприятия, т.к. в современной работе специалистов по защите информации помимо конфиденциальности, целостности и доступности требуется обеспечить еще и подотчетность. Под источником событий понимается любое программное или программно–аппаратное решение, обеспечивающие ведение журнала регистрации событий (журнала аудита), например, средство защиты информации, средства контроля и анализа защищенности и т.п. Сформулирована задача определения регистрируемых событий на источнике событий. Рассмотрены существующие способы определения набора регистрируемых событий на источнике событий и выявлены их недостатки. Выявлено противоречие между потребностями практики в необходимости наличия определенных зарегистрированных событий для проведения их дальнейшего анализа и принятием решения о регистрации соответствующих событий. Предложен способ, учитывающий недостатки существующих подходов, а также возможности используемого на предприятии технического решения класса Security Information and Event Management по выявлению инцидентов информационной безопасности, а именно набор предустановленных в данном техническом решении правил выявления инцидентов информационной безопасности (правил корреляции событий). Для каждого правила выявления инцидентов информационной безопасности предлагается определить свой поднабор регистрируемых событий, в результате чего, определение итогового набора регистрируемых событий на источнике событий осуществляется путем объединения полученных поднаборов. Данный способ позволяет максимизировать число выявляемых техническим решением класса Security Information and Event Management инцидентов информационной безопасности на базе итогового набора регистрируемых событий.

***Ключевые слова**: процесс управления, источник событий, событие, SIEM–система, инцидент*

Введение

Проблема обеспечения информационной безопасности (ИБ) автоматизированных информационных систем не только не теряет своей актуальности на протяжении ряда десятилетий, но и стремительно развивается и выходит на один из первых планов в научно-практической деятельности. При этом в последние годы в работе специалистов по защите информации на первое место выходит не возможность предотвращения инцидентов ИБ, а готовность их своевременного выявления (детектирования) и расследования [11]. Данное обстоятельство требует обеспечить помимо конфиденциальности, целостности и доступности однозначное прослеживание действий любого субъекта доступа в автоматизированных информационных системах, т.е. подотчетность в рамках процесса управления событиями [1]. Стоит отметить, что на практике при реализации процесса управления событиями специалистами по защите информации основной акцент делается на технические решения класса Security Information and Event Management (SIEM) [2-5], а не на источники событий (средства защиты информации, средства контроля и анализа защищенности и т.п.), которые осуществляют непосредственную регистрацию событий (ведение журнала регистрации событий (журнала аудита)) и, как следствие, выступают основой для инфраструктуры управления событиями. В связи с этим задача определения регистрируемых событий на источниках событий является актуальной.

Существующие способы определения регистрируемых событий

На сегодняшний день существует несколько способов решения поставленной задачи, но в них выявлен ряд недостатков [6-7]:

Регистрировать абсолютно все события – может приводить к перерасходу ресурсов источни-

1 Кузнецов Александр Васильевич, Финансовый университет при Правительстве РФ, г. Москва, 1283_my@mail.ru.
2 Ненашев Сергей Михайлович, Финансовый университет при Правительстве РФ, г. Москва, snenashev@gmail.com.

ка событий (вплоть до полного отказа в работе), а также зашумляет работу SIEM-системы.

Регистрировать события, определенные на источнике событий «по умолчанию», – зачастую использует минимальный набор регистрируемых событий (вплоть до полного отсутствия регистрации событий) может не отражать потребности конкретного предприятия, и, как следствие, может приводить к пропуску ценных для ИБ предприятия событий.

Регистрировать события, выявленные по результатам опытной эксплуатации SIEM-системы, – учитывая нестатистическую природу возникновения событий, может приводить к пропуску ценных для ИБ предприятия событий по завершению опытной эксплуатации SIEM-системы.

Таким образом, возникает противоречие между потребностями практики в обеспечении SIEM-системы необходимыми событиями для проведения их дальнейшего анализа, в том числе выявления инцидентов ИБ, и необходимостью принятия решения о регистрации данных событий на источнике событий, т.е. определения перечня регистрируемых событий.

Предлагаемый способ определения регистрируемых событий

Для каждого источника событий существует максимальный набор событий, которые могут быть зарегистрированы данным источником, – счетное множество E (1):

$$E_{max} = \{e_1, \ldots, e_m\}. \quad (1)$$

В SIEM-системе существует счетное множество предустановленных правил выявления инцидентов ИБ – I (2):

$$I = \{i_1, \ldots, i_n\}. \quad (2)$$

Возникает следующая задача определения счетного подмножества $Einc \subseteq Emax$, максимизирующего количество выявляемых инцидентов ИБ – W, на базе счетного множества I (3), т.е. $E_{inc} = \{e_p, \ldots, e_q\}$, где $p \geq 1$ и $q \leq m$, при которых выполняется условие (3):

$$W = \sum_{k=1}^{n} i_k(e_j) \rightarrow max. \quad (3)$$

Считая, что существуют счетные подмножества E_k, которые необходимы для срабатывания определенного правила i_k [8], предлагается решить обратную задачу, т.е. определить все события e_j, влияющие на срабатывание i_k правила, путем анализа правил в SIEM-системе с учетом принятого языка (синтаксиса) описания данных правил. После этого необходимо провести объединение полученных подмножеств Ek для каждого правила, получив итоговое счетное подмножество E_{inc} (4):

$$E_{inc} = \bigcup_{k=1}^{n} E_k \ . \quad (4)$$

Таким образом, способ определения регистрируемых событий включает в себя:

Определение множества правил выявления инцидентов ИБ в SIEM-системе – I.

Установления подмножеств событий для каждого правила выявления инцидентов ИБ в SIEM-системе – E_k, где $k \in [1;n]$.

Объединение полученных подмножеств событий с целью получения итогового подмножества – E_{inc}.

Выводы

Предложенный способ, учитывает недостатки существующих подходов, принимает во внимание возможности конкретной SIEM-системы по выявлению инцидентов ИБ, а именно предустановленные наборы правил выявления инцидентов ИБ (правил корреляции событий), и позволяет максимизировать число выявляемых инцидентов ИБ для конкретного предприятия.

Достоверность результатов подтверждается корректным использованием теоретических методов, а также тем, что предложенный способ получил практическое подтверждение на базе информационно-телекоммуникационной инфраструктуры научно-технического центра «Вулкан».

Данный способ является инвариантным к реализации автоматизированных информационных систем и SIEM-систем, что позволяет применять его в различных информационно-телекоммуникационных инфраструктурах. Дополнительно стоит отметить, что данный способ может быть перенесен для решения задач в других научно-практических областях, например, в области сбора и анализа данных в социальных сетях с целью определения информационного влияния в них [9-10].

Научный руководитель: Шеремет Игорь Анатольевич, доктор технических наук, профессор, i.a.sher@yandex.ru

Литература:

1. Кузнецов А.В. Способ организации процесса управления событиями, в части их обработки, в рамках системы управления информационной безопасностью предприятия // Вопросы защиты информации. 2015. № 2. 57-62 с.
2. D. Miller, S. Harris, A. Haeper, S. VanDyke, C. Blask. Security Information and Event Management (SIEM) Implementation. The McGraw-Hill. 2010.
3. Кузнецов А.В. RSA enVision – эффективный инструмент для работы с журналами событий Microsoft Windows. // Windows IT Pro/ RE. 2012. № 10. С. 56.
4. Марков А., Фадин А. Конвергенция средств защиты информации // Защита информации. Инсайд. 2013. № 4 (52). С. 80-81.
5. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах. // Труды СПИИРАН. 2012. № 1 (20). С. 27-56.
6. Райс А., Рингольд Д. Защита от целенаправленных устойчивых угроз с помощью больших данных. // Безопасность ИТ-инфраструктуры, 2015. № 4 (94). С. 6-7.
7. Чувакин А. SIEM: что делать, если некуда идти? // Безопасность ИТ-инфраструктуры, 2015. № 2 (92). С. 9–11.
8. Бирюков А. Security Operation Center. Искусственный интеллект на службе ИБ. // Системный администратор. 2013, № 9 (130). С. 42-45.
9. Кузнецов А.В., Ненашев С.М. Выявление узлов оптимального осуществления информационного влияния в социальных сетях. СПб: Межвузовский сборник трудов III Всероссийской научно-технической конференции ИКВО НИУ ИТМО, 2012. С.112–114.
10. Gupta R., Brooks H. Using Social Media for Global Security. John Wiley & Sons, Inc., 2013, pp.141–145.
11. Шеремет И.А. Угрозы техносфере России и противодействие им в современных условиях // Вестник академии военных наук. 2014. № 1 (46). С. 27-34.

METHOD OF SELECTION OF REGISTERED EVENTS

Kuznetcov A.V.[3], Nenashev S.M.[4]

Abstract. In this article the event source, which to register events, is considered as a basis for event management infrastructure within information security management system, due to information security specialists have to ensure accountability in additional to confidentiality, integrity and availability. Event source is any software or fareware ensuring security audit, for instance, security tools, control and analysis tools, etc. Formulated the problem to selection of registered events. Examined existing ways of selection of registered events and identified their weaknesses. Identified the contradiction between the requirements of practice as to the need for certain registered events for further analysis and making decision related to registration of relevant events. The method takes into account the weaknesses of existing approaches and capabilities used Security Information and Event Management system to identify information security incidents in the company, namely the set of preinstalled in this system rules for identification of information security incidents (rules of events correlation). For each rule to determine a subset of registered events, as a result, the final set of registered events on the event source is combination of obtained subsets. This method allows to increase number of detected information security incidents using Security Information and Event Management system and based on final set of registered events.

***Keywords**: management process, event source, event, SIEM system, incident*

References:

1. Kuznetcov A.V. Sposob organizatsii protsessa upravleniya sobytiyami, v chasti ikh obrabotki, v ramkakh sistemy upravleniya informatsionnoy bezopasnost'yu predpriyatiya. M: Voprosy zashchity informatsii, No 2, 2015, pp.57–62.
2. D. Miller, S. Harris, A. Haeper, S. VanDyke, C. Blask. Security Information and Event Management (SIEM) Implementation. The McGraw-Hill. 2010.
3. Kuznetcov A.V. RSA enVision – effektivnyy instrument dlya raboty s zhurnalami sobytiy Microsoft Windows. M: Windows IT Pro/ RE № 10, 2012. 56–57 p.
4. Markov A., Fadin A. Konvergentsiya sredstv zashchity informatsii, Zashchita informatsii. Insayd, 2013, No 4 (52), pp. 80-81.
5. Kotenko I.V., Saenko I.B., Polubelova O.V., Chechulin A.A. Primenenie tekhnologii upravleniya informatsiey i sobytiyami bezopasnosti dlya zashchity informatsii v kriticheski vazhnykh infrastrukturakh. M: Trudy SPIIRAN. Vyp. 1 (20), 2012. 27–56 p.
6. Rays A., Ringol'd D. Zashchita ot tselenapravlennykh ustoychivykh ugroz s pomoshch'yu bol'shikh dannykh. M: Bezopasnost' IT-infrastruktury № 4 (94), 2015. 6–7 p.
7. Chuvakin A. SIEM: chto delat', esli nekuda idti? M: Bezopasnost' IT-infrastruktury № 2 (92), 2015. 9–11 p.
8. Biryukov A. Security Operation Center. Iskusstvennyy intellekt na sluzhbe IB. M: Sistemnyy administrator № 9 (130), 2013. 42–45 p.
9. Kuznetcov A.V., Nenashev S.M. Vyyavlenie uzlov optimal'nogo osushchestvleniya informatsionnogo vliyaniya v sotsial'nykh setyakh. SPb: Mezhvuzovskiy sbornik trudov III Vserossiyskoy nauchno-tekhnicheskoy konferentsii IKVO NIU ITMO, 2012. 112–114 p.
10. Gupta R., Brooks H. Using Social Media for Global Security. John Wiley & Sons, Inc., 2013. 141–145 p.
11. Sheremet I.A. Ugrozy tekhnosfere Rossii i protivodeystvie im v sovremennykh usloviyakh, Vestnik akademii voennykh nauk. 2014, No 1 (46), pp. 27-34.

3 Aleksandr Kuznetsov, Financial University under the Government of the Russian Federation, Moscow, 1283_my@mail.ru.

4 Sergey Nenashev, Financial University under the Government of the Russian Federation, Moscow, snenashev@gmail.com.