УДК 004.056

НАСТРОЙКА АУДИТА БЕЗОПАСНОСТИ В ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА WINDOWS

Смотрук Г.С.

гр.367241

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Петров С.Н. – кандидат технических наук, доцент

Аннотация. Рассмотрены настройки аудита безопасности в операционных система семейства Windows в соответствии с законодательством Республики Беларусь. Правильно настроенный аудит безопасности играет важную роль для обеспечения информационной безопасности.

Ключевые слова: приказ Оперативно-аналитического центра № 130, аудит информационной безопасности, операционные системы

Введение. Двадцать пятого июля 2023 года вышел Приказ Оперативно-аналитического центра при президенте Республики Беларусь № 130 «О мерах по реализации Указа президента Республики Беларусь от 14 февраля 2023 г. № 40» [1]. В нем подробно описаны условия, необходимые для обеспечения информационной безопасности, формализованы алгоритмы действий при возникновении киберинцидентов, описаны требования к центрам кибербезопасности и их типовая структура.

Приказом определен перечень типов и записей событий информационной безопасности, которые должны централизованно собираться, обрабатываться, накапливаться, систематизироваться и храниться не менее одного года (далее – перечень). А их сбор должен осуществляться в круглосуточном режиме.

Основная часть. Для операционных систем вышеуказанный перечень выглядит следующим образом: запуск и (или) остановка системы; запуск и (или) остановка процессов; подключение съемных машинных носителей информации; подключение иных периферийных устройств к портам ввода (вывода) (мобильные устройства, сетевые адаптеры, беспроводные модемы и иные); установка и удаление программного обеспечения (изменение компонентов программного обеспечения); аутентификация (вход и (или) выход) пользователей в операционной системе, успешные и неуспешные попытки аутентификации; использование привилегированных учетных записей пользователей; создание, удаление, модификация учетных записей пользователей; неудавшиеся или отмененные действия пользователя и (или) процессы; создание или изменение параметров заданий в планировщике задач; установка, удаление, перезапуск, ошибка запуска службы и (или) сервиса; изменение системной конфигурации, в том числе сетевых настроек и средств межсетевого экранирования; изменение или попытки изменения настроек и средств управления защитой системы, в том числе антивирусного программного обеспечения, систем обнаружения и предотвращения вторжений; контроль несанкционированных сетевых соединений, в том числе попыток несанкционированного удаленного доступа, создания общих сетевых ресурсов, использования нестандартных сетевых портов.

В соответствии с вышеуказанным перечнем сформирована политика аудита [2], представленная в Таблице 1.

Таблица 1 – Политика аудита безопасности ОС Windows

Категория аудита безопасности	Идентификаторы событий и их описание
Аудит изменения состояния безопасности	4608: Windows запускается 4609: завершение работы Windows 4616: системное время было изменено 4621: администратор восстановил систему из CrashOnAuditFail
Аудит создания процессов	4688: создан новый процесс 4696: процессу был назначен первичный маркер
Аудит завершения процессов	4689: процесс завершился
Аудит съемного носителя	4656: запрошен дескриптор объекта 4658: дескриптор объекта закрыт 4663: предпринята попытка доступа к объекту
Аудит активности PNP	6416: новое внешнее устройство было распознано системой 6419: был сделан запрос на отключение устройства 6420: устройство было отключено 6421: был сделан запрос на включение устройства 6422: устройство было включено 6423: установка этого устройства запрещена системной политикой 6424: установка этого устройства была разрешена, после того как ранее было запрещено политикой
Аудит событий, создаваемых приложениями	4665: предпринята попытка создать контекст клиента приложения 4666: приложение попыталось выполнить операцию 4667: удален контекст клиента приложения 4668: приложение инициализировано 7045: в системе установлена служба 11724: удаление успешно завершено
Аудит входа в систему	4624: учетная запись успешно выполнена 4625: не удалось войти в учетную запись 4648: предпринята попытка входа с использованием явных учетных данных 4675: идентификаторы безопасности были отфильтрованы
Аудит выхода из системы	4634: процесс выхода был завершен для пользователя 4647: инициированный пользователем выход
Аудит проверки учетных данных	4774: учетная запись была сопоставлена для входа 4775: не удалось сопоставить учетную запись для входа 4776: компьютер пытался проверить учетные данные для учетной записи 4777: контроллер домена не смог проверить учетные данные для учетной записи
Аудит специального входа	4964: для нового входа назначены специальные группы 4672: специальные привилегии, назначенные новому входу
Аудит управления учетными записями пользователей	4720: создана учетная запись пользователя 4722: учетная запись пользователя включена 4723: предпринята попытка изменить пароль учетной записи 4724: предпринята попытка сброса пароля учетной записи 4725: учетная запись пользователя отключена 4726: учетная запись пользователя удалена 4738: учетная запись пользователя была изменена 4740: учетная запись пользователя заблокирована 4765: журнал безопасности был добавлен в учетную запись 4766: попытка добавить журнал идентификаторов безопасности в учетную запись завершилась ошибкой

Категория аудита безопасности	Идентификаторы событий и их описание
	4767: учетная запись пользователя была разблокирована 4780: список ACL был установлен для учетных записей, которые являются членами групп администраторов 4781: имя учетной записи было изменено
Аудит доступа к службе каталогов	4662: с объектом выполнена операция 4661: запрошен дескриптор объекта
Аудит других событий доступа к объектам	4691: запрошен косвенный доступ к объекту 5148: платформа фильтрации Windows обнаружила DoS-атаку и вошла в оборонительный режим; пакеты, связанные с этой атакой, будут отброшены 5149: атака DoS утихла, и нормальная обработка возобновляется 4698: была создана запланированная задача 4699: запланированная задача удалена 4700: была включена запланированная задача 4701: запланированная задача отключена 4702: запланированная задача обновлена
Аудит других системных событий	5030: не удалось запустить службу брандмауэра Windows
Аудит расширения системы безопасности	4697: в системе была установлена служба
Аудит целостности системы	4612: внутренние ресурсы, выделенные для постановки сообщений аудита, исчерпаны, что привело к потере некоторых аудитов
Аудит изменения политики на уровне правил MPSSVC	4944: при запуске брандмауэра Windows была активна следующая политика 4945: при запуске брандмауэра Windows было указано правило 4946: в список исключений брандмауэра Windows внесено изменение (было добавлено правило) 4947: в список исключений брандмауэра Windows внесено изменение. (правило было изменено) 4948: в список исключений брандмауэра Windows внесено изменение. (правило было удалено) 4949: параметры брандмауэра Windows были восстановлены до значений по умолчанию 4950: параметр брандмауэра Windows изменен 4951: правило было проигнорировано, так как его основной номер версии не распознан брандмауэром Windows 4956: брандмауэр Windows изменил активный профиль 4957: брандмауэр Windows не применял следующее правило 4958: брандмауэр Windows не применил следующее правило, так как оно ссылается на элементы, не настроенные на этом компьютере
Аудит изменения состояния безопасности	4616: системное время было изменено
Аудит изменения политики аудита	4715: политика аудита (SACL) для объекта была изменена 4719: политика аудита системы была изменена 4817: параметры аудита объекта были изменены

Категория аудита безопасности	Идентификаторы событий и их описание
	4902: создана таблица политик аудита для каждого пользователя 4906: значение CrashOnAuditFail изменилось 4907: параметры аудита объекта были изменены 490: таблица входа в специальные группы изменена 4912: политика аудита на пользователя была изменена 4904: предпринята попытка зарегистрировать источник событий безопасности 4905: предпринята попытка отменить регистрацию источника событий безопасности
Аудит изменения политики проверки подлинности	4670: изменены разрешения для объекта 4706: для домена было создано новое доверие 4707: удалено доверие к домену 4716: сведения о доверенном домене были изменены 4713: политика Kerberos была изменена 4717: доступ к системной безопасности был предоставлен учетной записи 4718: доступ к системной безопасности был удален из учетной записи 4739: политика домена изменена 4864: обнаружен конфликт пространства имен 4865: добавлена запись сведений о доверенном лесе 4866: удалена запись сведений о доверенном лесе 4867: изменена запись сведений о доверенном лесе
Аудит общего файлового ресурса	5140: доступ к объекту сетевой общей папки 5142: добавлен объект сетевой общей папки 5143: объект сетевой общей папки был изменен 5144: объект сетевой общей папки был удален 5168: сбой проверки имени субъекта-службы для SMB/SMB2

Правильно настроенный аудит безопасности является неотъемлемой частью комплексной стратегии информационной безопасности. Преимущества правильно настроенного аудита безопасности:

Обнаружение угроз и реагирование на инциденты: аудит позволяет организациям отслеживать и регистрировать все важные события безопасности. Это помогает выявлять подозрительную активность, такую как несанкционированные попытки входа в систему или изменения в критических системных файлах, что позволяет организациям быстро реагировать на потенциальные угрозы.

Выявление уязвимостей и улучшение безопасности: аудит помогает выявлять уязвимости в системе безопасности и принимать меры по их устранению, повышая общую эффективность информационной безопасности.

Предотвращение потерь и финансовых последствий: эффективный аудит помогает предотвращать нарушения безопасности и минимизировать их последствия, защищая организации от потерь данных, финансовых потерь и репутационного ущерба.

Заключение. Правильно настроенный аудит безопасности позволяет выбирать главные и нужные события безопасности, подлежащие централизованной консолидации для последующего обращения к ним при расследовании инцидентов информационной безопасности. Это помогает избежать сбора ненужных событий, которые могут перегрузить систему и затруднить выявление реальных угроз. Внедрение и правильная настройка аудита безопасности должны быть приоритетом для всех организаций, стремящихся защитить свои информационные активы.

Список литературы

4. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь № 130 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40». [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2023%20-%20130.pdf. – Дата доступа: 15.02.2024.

5. Параметры политики расширенного аудит безопасности Windows. [Электронный ресурс]. – Режим доступа: https://learn.microsoft.com/ru-ru/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings – Дата доступа: 15.02.2024.

UDC 004.056

SETTING UP A SECURITY AUDIT IN WINDOWS OPERATING SYSTEMS

Smotruk H.S.

gr. 367241

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Petrov S.N. – PhD, associate professor

Annotation. The settings for security audits in operating systems of the Windows family are considered in accordance with the legislation of the Republic of Belarus. A properly configured security audit plays an important role in ensuring information security.

Keywords: Order of the Operational Analytical Center No. 130, information security audit, operating systems