

*Махлин Борис Михайлович, студент 2 курс магистратуры, кафедра
«Железнодорожная автоматика, телемеханика и связь», Российский
университет Транспорта (МИИТ), Россия, г. Москва*

ЕДИНАЯ СИСТЕМА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ КОМПАНИИ КАК СОВРЕМЕННОЕ СРЕДСТВО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: Статья посвящена проблеме соответствия компании современным требованиям по обеспечению информационной безопасности. Автор раскрывает современные способы организации процессов мониторинга, анализа, выявления нарушений, уязвимостей информационных систем, позволяющие снизить ущерб от возникающих инцидентов и уменьшить затраты на контроль событий информационной безопасности при этом в целом повышая уровень защищённости компании.

Ключевые слова: мониторинг, инцидент, инфраструктура, анализ информации, аномальная активность.

Abstract: The article is devoted to the problem of compliance of the company with modern requirements for ensuring information security. The author reveals modern ways of organizing monitoring, analysis, detection of violations, vulnerabilities of information systems, which can reduce the damage from incidents and reduce the cost of monitoring information security events while generally increasing the level of security of the company.

Key words: monitoring, incident, infrastructure, information analysis, abnormal activity.

Современные требования обеспечения информационной безопасности, соблюдение законов (таких как №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [3] и др.), ставят перед компаниями новые цели и задачи по обеспечению безопасности информации, которая хранится, обрабатывается и передаётся как внутри компании, так и во внешнем мире. В каждой компании, независимо от её размера, существует собственная информационная система. Она может быть, как простой, так и сложносоставной и все её части необходимо защищать по одним и тем же принципам:

1. Организационные меры;
2. Превентивные меры;
3. Средства наблюдения, обнаруживающие аномальную активность;
4. Инструменты и средства реагирования;
5. Использование человеческого ресурса.

Последний пункт задействуется далеко не всегда, т.к. проблему безопасности возможно решить с помощью автоматических методов. У каждой компании применяются свои наработанные инструменты организации безопасности компонентов информационной системы, но в последнее время, стала прослеживаться общая тенденция. Большая часть компаний приходят к решению о внедрении центров управления информационной безопасностью, Security Operations Center (SOC).

Что же такое Security Operations Center (SOC)? SOC объединяет между собой все процессы и компоненты, обеспечивающие информационную безопасность организации, формируя цельную, понятную и предельно детализированную картину текущей ситуации. Основой SOC является система управления событиями информационной безопасности, Security information and event management (SIEM). SIEM — это система, предназначенная для сбора, анализа информации из других систем, таких как Антивирусы, маршрутизаторы, IDS, DLP и пр., собирающая логи с web-серверов, тонких и толстых клиентов и других устройств, и компонентов информационной системы, позволяя выявлять отклонения от нормальных параметров по определённым критериям. Как только появилось расхождение данных, создаётся инцидент. Основная функция SIEM – приведение к общему формату огромного количества логов от различных источников для повышения удобства опрaвления и обнаружения взаимосвязей между ними. Сама по себе SIEM не несёт никаких функций по обеспечению защиты [2].

Таким образом, SOC не просто модернизирует систему информационной безопасности организации, но является инструментом, в целом повышающим уровень защищённости компании. Применение SOC позволяет проводить:

- сбор и анализ событий существующих информационных систем;
- инвентаризацию инфраструктурных компонентов;
- выстраивание зависимости событий информационной безопасности;

- упорядочивание информации и её оперативную передачу для расследования инцидентов информационной безопасности;
- снижение времени реакции на инциденты информационной безопасности;
- формирование отчётов и структурный анализ информации по инцидентам.

SOC и его функционал, позволяют компании отслеживать уязвимые места информационной системы и модернизировать их, совершенствуя меры защиты, снижать расходы за счёт минимизации ущерба от возникающих инцидентов и уменьшить затраты на контроль событий информационной безопасности и аудит сторонних организаций. Подобные улучшения в свою очередь приводят к глобальным общекорпоративным преимуществам, таким как стабильность и прозрачность бизнес-процессов компании, эффективность и управляемость информационной безопасности, что влечёт за собой повышение безопасности и устойчивости бизнеса.

Существуют основные этапы создания SOC:

- обследование защищаемой инфраструктуры компании, как на техническом, так и на организационном уровне;
- установка и настройка всех необходимых средств мониторинга и защиты;
- выбор подходящей SIEM и её настройка под каждую отдельно взятую компанию;
- создание правил выстраивания зависимости событий;
- подбор персонала по работе с SOC. В их обязанности будет входить проведение мониторинга событий [1], внесение исправлений в правила выстраивания их зависимости от тех или иных факторов, реагирование на события безопасности. Это команда, состоящая в основном из аналитиков по информационной безопасности, в задачи которой входит обнаружение и анализ инцидентов кибербезопасности, оперативное реагирование, предотвращение их возникновения и составление отчетности.

Существует перспективное направление SOC – оказание облачных услуг, включающее в себя:

- подключение инфраструктуры клиентов к собственному SOC;
- постоянный мониторинг и исследование событий информационной безопасности;
- мгновенное реагирование в режиме 24x7 на инциденты информационной безопасности;
- формирование регулярных отчетов для технических специалистов отделов информационной безопасности и руководства компании.

С помощью SOC реализуются нормативные и международные требования по обеспечению информационной безопасности компании.

Библиографический список:

1. Бондарев В.В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства: учеб. пособие. – М.: МГТУ им. Н. Э. Баумана, 2017. – 228 с.
2. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учеб. пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой – М.: Горячая линия–Телеком, 2014. – 170 с.
3. Федеральный закон N 187-ФЗ от 26.07.2017. О безопасности критической информационной инфраструктуры Российской Федерации. – 2017 [Электронный ресурс]. КонсультантПлюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 17.10.2019).