МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**



**МОСКОВСКИЙ**

**ПОЛИТЕХ**

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра «Информационная безопасность»

Проектная деятельность

Тема: “Оценка зрелости фреймворка **CIS Critical Security Controls**”

Выполнил: Студент 2 курса гр. 191-331

Юрин Даниил Романович

Научный руководитель:

Агеева Елена Александровна

2020 г. Москва

**Содержание:**

Вступление………………………………………………………………………..2

**Часть 1**…………………………………………………………………………....4

Этап 1: Модель CIS Controls V7……………….………...………………..4

Этап 1: Элементы управления безопасностью………………………...…7

Вывод………………………………………………..………………………9

**Часть 2**…………………………………………………………………………10

**CIS Control 1**……………………………………………..…………….10

**CIS Control 2**……………………………………………..…………….12

**CIS Control 3**……………………………………………..…………….14

**CIS Control 4**………………………………………………..………….16

**CIS Control 5**………………………………………………..………….18

**CIS Control 6**…………………………………………………..……….19

**CIS Control 7**…………………………………………………..……….21

**CIS Control 8**…………………………………………………..……….23

**CIS Control 9**…………………………………………………..……….25

**CIS Control 10**………………………………………………………….25

**CIS Control 11**………………………………………………………….27

**CIS Control 12**………………………………………………………….29

**CIS Control 13**………………………………………………………….31

**CIS Control 14**………………………………………………………….32

**CIS Control 15**………………………………………………………….34

**CIS Control 16**………………………………………………………….36

**CIS Control 17**………………………………………………………….38

**CIS Control 18**………………………………………………………….40

**CIS Control 19**………………………………………………………….42

**CIS Control 20**………………………………………………………….44

**Вывод**……………………………...…………………………………….46

**Часть 1.**

**Вступление:**

Информационная безопасность компании, общественной организации или производственного предприятия – это комплекс мероприятий, направленных на предотвращение несанкционированного доступа к внутренней IT-инфраструктуре, незаконного завладения конфиденциальной информацией и внесения изменений в базы данных. [Википедия](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C) включает в это понятие любые формы данных, независимо от их материального представления. То есть, в информационную безопасность входит защита от злоумышленников данных в электронной форме и на физических носителях.

Учитывая важность информации в современном мире, защите от утечек конфиденциальной информации в адрес конкурентов необходимо уделять повышенное внимание. Возможный ущерб может быть намного большим, чем стоимость всех материальных активов предприятия. Именно поэтому, современные организации используют специальные фреймворки по защите своих данных.

Существует множество различных фреймворков, предоставляемых на рынке защиты информации, но самый известный из них - это **CIS Controls V7**. Принцип работы которого мы сейчас и рассмотрим.

**Этап 1.**

**Модель CIS Controls V7.**

Модель «**CIS Critical Security Controls**», была разработана ведущими экспертами института **SANS**, объединившими свои колоссальные знания и навыки в области кибербезопасности.

Они создали обширный список средств контроля данных в интернете, представляющий собой лучшие методы защиты от киберпреступности.

Данные методы гарантируют, что средства управления **CIS** являются наиболее эффективными мерами защиты, обеспечивающими сохранность данных компаний, как от наиболее известных и распространенных кибератак в сети, так и от самых сложных и менее популярных способов кражи.

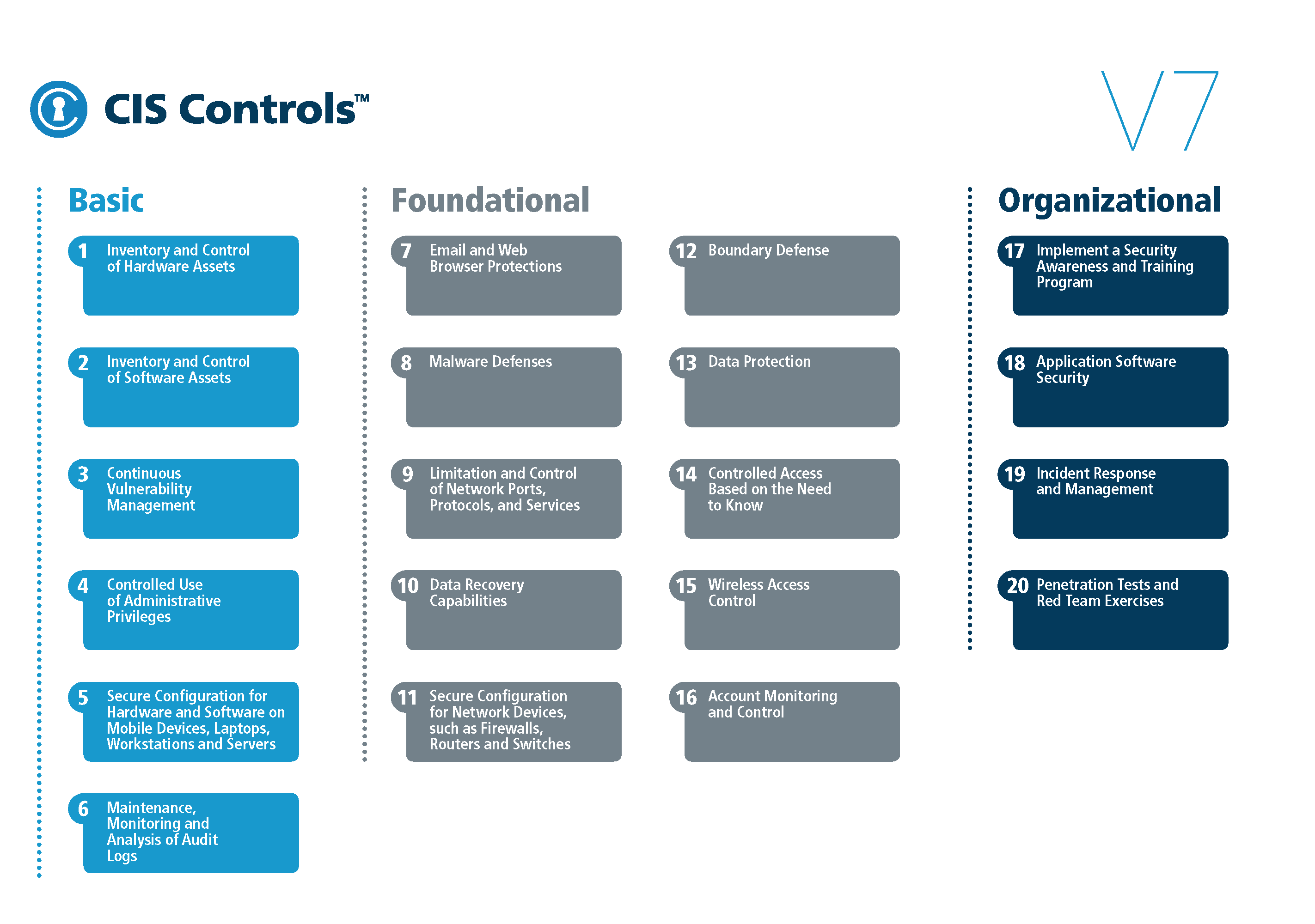
Для этого **CIS** разработало **пять** важнейших принципов работы эффективной системы киберзащиты:

1. **Offense informs defense (**Нападение информирует защиту**).** Суть этого принципа заключается в том, что используются знания о реальных атаках, произведённых на системы. Это нужно для того, чтобы обеспечить эффективность работы средств защиты.
2. **Prioritization** (Определение приоритетов). Суть данного принципа заключается в том, что сначала устанавливаются те средства управления системой, которые смогут обеспечить максимальное снижение рисков потери данных от наиболее опасных угроз. Помимо этого, происходит установка только тех систем, которые могут быть реально реализованы в вашей вычислительной среде. Не нужно тратить средства на те системы, которые не принесут максимальную защиту от киберугроз и не смогут корректно работать в вашей среде.
3. **Measurements and Metrics** (Измерения и метрики). Суть этого принципа заключается в том, что устанавливаются единые показатели, чтобы руководители, ИТ-специалисты, аудиторы и сотрудники службы безопасности использовали общий язык для измерения эффективности мер безопасности в организации. Это нужно для того, чтобы можно в дальнейшем легко производить необходимые корректировки в системе.
4. **Continuous diagnostics and mitigation** (Непрерывная диагностика и устранение неполадок). Суть данного принципа заключается в том, что все время должно выполняться непрерывное тестирование эффективности работы текущих мер защиты и обеспечения безопасности.
5. **Automation** (Автоматизация). Суть данного принципа заключается в том, что производится автоматизация средств защиты.

Помимо этого, **CIS** разделило меры защиты от кибератак на специальные группы реализации **IG1**, **IG2,** **IG3**:

* [](https://4.bp.blogspot.com/-_8xUuNXmfTM/XKsR4J4vmSI/AAAAAAAAa5Y/SvXhgUooVawGDEuviejMUKmVDbhCkVyfgCLcBGAs/s1600/IG1.png)**Implementation group 1 - IG1.** Организации, применяющие **IG1** – в основном малый (иногда средний бизнес), с ограниченным опытом в ИТ и кибербезопасности. Основная задача этих организаций - сохранить бизнес в рабочем состоянии, а основной ущерб - от простоя.  Как правило обрабатывают не критичные данные своих сотрудников и финансовую информацию. Если же организации малого бизнеса обрабатывают критичные данные, то должны выполнять меры следующих групп. Меры защиты, реализуемые в рамках группы **IG1**, должны осуществляться в варианте, требующем минимум компетенций в области ИБ и рассчитаны на коробочные решения оборудования и ПО для малого бизнеса.
* [](https://3.bp.blogspot.com/-w380mOVKrzU/XKsR4FLUFiI/AAAAAAAAa5U/9F2bU7sO14EZ2U8KKkUtGLtzMA9BpXsagCLcBGAs/s1600/IG2.png)**Implementation group 2 – IG2.** В организациях, применяющих **IG2** как правило есть выделенные работники, отвечающие за управление ИБ и защиты ИТ инфраструктуры. В таких организациях есть процессы и подразделения разной степени критичности. Некоторые подразделения могут быть нацелены в первую очередь на выполнение требований законодательства (**compliance**). Организации группы **IG2** как правило обрабатывают важную информацию своих клиентов и контрагентов и устойчивы к коротким перерывам в обслуживании. Основное беспокойство вызывает потеря репутации в случае инцидентов. Частные меры группы **IG2**, помогают ответственным за безопасность лицам, справляться с возрастающей сложностью процессов и операций. Установки и настройки некоторых меры будут зависеть от имеющегося в компании уровня технологий и экспертизы.
* [https://1.bp.blogspot.com/-_p372dmE1dY/XKsR4H724mI/AAAAAAAAa5c/-enwRSA72bMsjQxMhYMBvrALwj5k0mwDQCLcBGAs/s200/IG3.png](https://1.bp.blogspot.com/-_p372dmE1dY/XKsR4H724mI/AAAAAAAAa5c/-enwRSA72bMsjQxMhYMBvrALwj5k0mwDQCLcBGAs/s1600/IG3.png)**Implementation group 3 – IG3.** В организациях группы **IG3** тысячи работников, в том числе имеются эксперты по безопасности, которые специализируются на различных аспектах кибербезопасность (например, управление рисками, тестирование на проникновение, безопасность приложений). Системы и данные организаций группы **IG3** содержат конфиденциальную информацию или функции, которые строго регулируются или должны соответствовать требованиям. Организации группы **IG3** должны обеспечивать доступность услуг, конфиденциальность и целостность данных. Успешные атаки могут нанести большой вред обществу. Меры защиты, выбранные для **IG3**, направлены на противодействие целевым и новым атакам от нарушителей с высоким потенциалом.

**Элементы управления безопасностью.**

Описание критических элементов управления безопасностью включает в себя всесторонние проверки элементов ИТ-инфраструктуры, конфигураций, прав доступа, привилегий, системных журналов, мер и средств реагирования на инциденты и инициирование проверок.  
В 7 редакции руководства элементы распределены на три категории, учитывающие современный ландшафт киберугроз.  


**Базовые.**  
В этой категории содержатся рекомендации, необходимые для обеспечения информационной безопасности организации. В эту категорию входят следующие пункты:

* инвентаризация авторизированных и неавторизованных устройств;
* инвентаризация авторизированного и неавторизованного программного обеспечения;
* средства управления уязвимостями;
* использование административных привилегий;
* защищенные конфигурации для мобильных устройств, ноутбуков, АРМ и серверов;
* обслуживание, мониторинг и анализ журналов аудита.

**Фундаментальные.**  
В эту категорию входят рекомендации, необходимые для применения лучших практик для обеспечения преимуществ и использования передовых технологий кибер-безопасности. В эту категорию входят следующие пункты:

* защита электронной почты и веб-браузера;
* защита от вредоносных программ;
* ограничение и контроль сетевых портов;
* возможность восстановления данных;
* защищенные конфигурации для сетевых устройств;
* защита периметра;
* защита данных;
* контроль доступа к данным;
* контроль доступа беспроводных сетей;
* контроль учетных записей.

**Организационные**.  
В эту категорию входят рекомендации, ориентированные на организационные процессы и административные меры, связанные с обеспечением информационной безопасности, с целью повышения осведомленности персонала и проведения Red Team/Blue Team операций. В эту категорию входят следующие пункты:

* контроль уровня осведомленности персонала;
* контроль прикладного программного обеспечения;
* реагирование на инциденты;
* тестирование на проникновение/Red Team.

Эти рекомендации позволяют составить четкие и приоритетные руководства для решения задач по обеспечению информационной безопасности организации и могут быть использованы как основа политик информационной безопасности.

**Вывод.**  
Модель **CIS Controls V7** была разработана для любых типов организаций, коммерческих фирм, неправительственных организаций, производственных предприятий:

* Применима к любой организации независимо от размера, контекста и ресурсов;
* Требует высокой квалификации менеджеров по безопасности и высокой детализации процессов безопасности;
* Позволяет организациям расположить по приоритетам и оптимизировать свои инвестиции в безопасность;

**Часть 2.**

#### **Control 1: Inventory and Control of Hardware Assets – Инвентаризация и контроль аппаратных средств.**

**Почему данный CIS важен?**

Злоумышленники, которые могут находиться в любой точке мира, непрерывно сканируют адресное пространство целевых организаций, ожидая подключения к сети новых и новых, незащищенных систем. Их особенно интересуют устройства, которые приходят и уходят из корпоративной сети, такие как ноутбуки или собственные устройства (BYOD), которые могут быть не синхронизированы с обновлениями безопасности или могут быть уже взломаны. Для атак используются новые устройства, которое были подключены к сети недавно вечером и их еще не успели настроить согласно регламенту безопасности корпорации. Даже устройства, которые не находятся в данный момент в Интернете, но были подключены к корпоративное сети, на которую хотят произвести атаку, могут быть использованы злоумышленниками для взлома. Именно поэтому **CIS Controls 1** очень важен, ведь он позволяет защитить корпорацию от кибератак через новые подключенные устройства к сети, а также он исключает несанкционированное подключение этих устройств к сети корпорации.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 1: Инвентаризация и контроль аппаратных средств.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 1.1 | Используется активный инструмент обнаружения. | Используются активные средства обнаружения устройств в сети для их идентификации в корпоративной сети интернет. Группы реализации: группа реализации 2 и группа реализации 3. | |
| 1.2 | Используется инструмент обнаружения пассивных активов. | Используется инструмент обнаружения пассивных активов для дальней идентификации устройств, подключенных к сети организации и автоматического обновления инвентаря организации. Группы реализации: группа реализации 3. | |
| 1.3 | Используется ведение журнала DHCP для последующего обновления инвентаризации активов. | Используется протокол динамической конфигурации хоста (DHCP) на всех DHCP-серверах или инструменты управления IP-адресами для того, чтобы обновить инвентарь оборудования организации. Группы реализации: группа реализации 2, группа реализации 3. | |
| 1.4 | Ведение подробного журнала инвентаризации активов. | Необходимо поддерживать точную и актуальную инвентаризацию всех технологических активов, которые могут хранить или обрабатывать информацию. Данный инвентарный список должен содержать все активы, независимо от того, подключены ли они к сети организации или нет. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 1.5 | Поддержание актуальной и подробной информации об активах корпорации. | Необходимо убедиться, что инвентаризация аппаратных активов записывает сетевой адрес, аппаратный адрес, имя машины, имя владельца актива данных и отдел для каждого актива, а также, информацию о том, одобрено ли устройства для его подключения к сети. Группы реализации: группа реализации 2, группа реализации 3. | |
| 1.6 | Контроль IP-адреса неавторизованных устройств. | Необходимо убедиться, что неавторизованные устройства либо удалены из сети, либо помещены в карантин. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 1.7 | Развернутый контроль доступа к сети на уровне порта. | Необходимо использовать контроль доступа на уровне порта, следуя стандартам **802.1x**, чтобы контролировать, какие устройства могут аутентифицироваться в сети. Система аутентификации должна быть привязана к данным инвентаризации аппаратных средств, чтобы гарантировать, что только авторизованные устройства могут подключаться к сети. Группы реализации: группа реализации 2, группа реализации 3. | |
| 1.8 | Используются клиентские сертификаты для аутентификации устройств. | Необходимо использовать клиентские сертификаты для аутентификации аппаратных средств, подключающихся к доверенной сети организации. Группы реализации: группа реализации 3. | |

#### **Control 2: Inventory and Control of Software Assets – Инвентаризация и контроль программных средств.**

**Почему данный CIS важен?**

Злоумышленники постоянно сканируют целевые организации в поисках уязвимых версий программного обеспечения. Помимо этого, они также распространяют вредоносные веб-страницы, файлы документов, медиа файлы и другой контент через свои собственные веб-страницы. Поэтому, когда ничего не подозревающие жертвы обращаются к этому контенту с помощью уязвимого браузера или другой клиентской программы, злоумышленники компрометируют их машины, часто устанавливая бэкдоры и ботов, которые дают им долгосрочный контроль над системой. Некоторые изощренные злоумышленники могут использовать эксплойты нулевого дня, которые используют ранее неизвестные уязвимости, для которых производитель программного обеспечения еще не выпустил патч. Именно поэтому данный **CIS Controls** очень важен для обеспечения комплексной защиты сети, ведь без надлежащих знаний невозможно должным образом обеспечить качественную защиту аппаратных средств, находящихся в корпоративной сети.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 2: Инвентаризация и контроль программных средств.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 2.1 | Ведение журнала инвентаризации авторизованного программного обеспечения. | Необходимо поддерживать актуальный список всего авторизованного программного обеспечения, которое требуется на предприятии для любых бизнес-целей в любой бизнес-системе. Группы реализации: группа реализации 1, группа реализации 2 и группа реализации 3. | |
| 2.2 | Проверка поддержки обновлений программного обеспечения поставщиком. | Необходимо убедиться, что в авторизованный реестр программного обеспечения организации добавлены только программные приложения или операционные системы, которые в настоящее время поддерживаются и получают обновления от поставщиков. Неподдерживаемое программное обеспечение должно быть помечено как неподдерживаемое в системе инвентаризации. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3 | |
| 2.3 | Автоматизация ведения инвентаризации программного обеспечения. | Необходимо используйте инструменты инвентаризации программного обеспечения по всей организации, чтобы автоматизировать документирование всего программного обеспечения в бизнес-системах. Группы реализации: группа реализации 2, группа реализации 3. | |
| 2.4 | Отслеживание инвентаризации программного обеспечения. | Система инвентаризации программного обеспечения должна отслеживать имя, версию, издателя и дату установки для всего программного обеспечения, включая операционные системы, авторизованные организацией. Группы реализации: группа реализации 2, группа реализации 3. | |
| 2.5 | Единость журнала инвентаризаций. | Система инвентаризации программного обеспечения должна быть связана с инвентаризацией аппаратных средств, чтобы все устройства и связанное программное обеспечение отслеживались из одного места. Группы реализации: группа реализации 3. | |
| 2.6 | Контроль авторизации программного обеспечения. | Необходимо убедиться, что неавторизованные программное обеспечение либо удалено из сети, либо помещено в карантин. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 2.7 | Использование технологии «Белый список». | Необходимо использовать технологию белых списков приложений для всех активов, чтобы гарантировать, что только авторизованное программное обеспечение будет работать, а все неавторизованное программное обеспечение заблокировано от выполнения действий на активах корпорации. Группы реализации: группа реализации 3. | |
| 2.8 | Правильная реализация технологии «Белый список». | Программное обеспечение организации для внесения в белый список приложений должно гарантировать, что только авторизованные библиотеки программного обеспечения (например, \* .dll, \* .ocx, \* .so и т. Д.) Могут загружаться в системный процесс. Группы реализации: группа реализации 3. | |
| 2.9 | Правильная реализации технологии «Белый список скриптов». | Программное обеспечение организации для внесения в белый список приложений должно гарантировать, что только авторизованные сценарии с цифровой подписью (например, \* .ps1, \*. Py, макросы и т. Д.) Могут выполняться в системе. Группы реализации: группа реализации 3. | |
| 2.10 | Использование физического или логического изолирования системы. | Следует использовать физически или логически изолированные системы для запуска программного обеспечения, которое требуется для бизнес-операций и имеет повышенный риск для организации. Группы реализации: группа реализации 3. | |

#### **Control 3: Continuous Vulnerability Management** **– Непрерывное управление уязвимостями.**

**Почему данный CIS важен?**

Киберзащитники должны работать в постоянно с новой информацией: это обновления программного обеспечения, маленькие исправления в системе, рекомендации по безопасности и т. д. Понимание уязвимостей и управление ими стало постоянной деятельностью, требующей значительного времени, внимания и ресурсов. Злоумышленники также имеют доступ к этой же информации и могут воспользоваться пробелами в защите системы, использующей новое ПО. Например, когда исследователи сообщают о новых уязвимостях, начинается гонка между всеми сторонами, в том числе: злоумышленниками (для «использования оружия», развертыванием атаки, эксплойта), поставщиками (для разработки, развертывания исправлений или сигнатур и обновлений) и защитников (для оценки риск, патчи регрессионного тестирования, установка). Организации, которые не сканируют уязвимости и не устраняют обнаруженные недостатки заранее, сталкиваются со значительной вероятностью компрометации своих компьютерных систем.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 3: Непрерывное управление уязвимостями.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 3.1 | Запуск автоматического сканирования уязвимостей. | Необходимо использовать современный инструмент сканирования уязвимостей, совместимый с протоколом автоматизации безопасности содержимого (SCAP), чтобы автоматически сканировать все системы в сети на еженедельной или более частой основе для выявления всех потенциальных уязвимостей в системах организации. Группы реализации: группа реализации 2 и группа реализации 3. | |
| 3.2 | Выполнять проверку результата подлинности сканирования уязвимостей. | Необходимо выполните сканирование уязвимостей с проверкой подлинности с помощью агентов, работающих локально в каждой системе, или с помощью удаленных сканеров, настроенных с повышенными правами в тестируемой системе. Группы реализации: группа реализации 2, группа реализации 3 | |
| 3.3 | Выделение отдельной учетной записи для проведения сканирования. | Необходимо использовать выделенную учетную запись для проверенного сканирования уязвимостей, которую не следует использовать для каких-либо других административных действий, и которая должна быть привязана к определенным машинам с определенными IP-адресами. Группы реализации: группа реализации 2, группа реализации 3. | |
| 3.4 | Развёртывание инструментов автоматического обновления программного обеспечения на уровне ОС. | Необходимо развернуть инструменты автоматического обновления программного обеспечения, чтобы убедиться, что в операционных системах используются самые последние обновления безопасности, предоставленные поставщиком программного обеспечения. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 3.5 | Развёртывание инструментов автоматического обновления программного обеспечения на уровне ПО. | Необходимо развернуть инструменты автоматического обновления программного обеспечения, чтобы гарантировать, что на стороннем программном обеспечении во всех системах установлены самые последние обновления безопасности, предоставленные поставщиком программного обеспечения. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 3.6 | Сравнение результатов сканирования. | Необходимо регулярно сравнивать результаты последовательного сканирования уязвимостей, чтобы убедиться, что уязвимости были устранены своевременно. Группы реализации: группа реализации 2, группа реализации 3. | |
| 3.7 | Использование процесса оценки риска. | Необходимо использовать процесс оценки риска, чтобы определить приоритетность устранения обнаруженных уязвимостей. Группы реализации: группа реализации 2, группа реализации 3. | |

#### **Control 4: Controlled Use of Administrative Privileges – Контролируемое использование административных привилегий.**

**Почему данный CIS важен?**

Злоупотребление административными привилегиями - это основной способ получения атак на целевое предприятие. Это связано с тем, что пользователя рабочей станции, работающего как привилегированный пользователь, обманывают, заставляя открыть вредоносное вложение электронной почты, либо загрузить и открыть файл с вредоносного веб-сайта или просто перейти на веб-сайт, на котором размещен контент злоумышленника. Файл или эксплойт содержит исполняемый код, который запускается на машине жертвы либо автоматически, либо путем обмана пользователя для выполнения содержимого злоумышленника. Если учетная запись пользователя жертвы имеет административные привилегии, злоумышленник может полностью захватить компьютер жертвы и установить регистраторы нажатий клавиш, снифферы, и программное обеспечение удаленного управления для поиска паролей администратора и других конфиденциальных данных. Поэтому очень важно контролировать использование работниками административных привилегий компании.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 4: Контроль использования административных привилегий.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 4.1 | Ведение журнала инвентаризации учетных записей. | Необходимо использовать автоматизированные инструменты для инвентаризации всех административных учетных записей, включая доменные и локальные учетные записи для того, чтобы гарантировать, что только авторизованные лица имеют повышенные привилегии. Группы реализации: группа реализации 2 и группа реализации 3. | |
| 4.2 | Изменение паролей по умолчанию. | Необходимо, перед развертыванием нового актива, изменить все пароли по умолчанию, чтобы они соответствовали значениям учетных записей административного уровня. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 4.3 | Разграничение учетных записей пользователей для различных привилегий доступа. | Необходимо убедиться, что все пользователи с доступом к административной учетной записи используют выделенную или дополнительную учетную запись для действий с повышенными правами. Эта учетная запись должна использоваться только для административных действий, а не для просмотра веб-страниц, электронной почты или аналогичных действий. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 4.4 | Использование уникальных паролей. | Если многофакторная проверка подлинности не поддерживается (например, учетные записи локального администратора, root или службы), учетные записи будут использовать пароли, уникальные для этой системы. Группы реализации: группа реализации 2, группа реализации 3. | |
| 4.5 | Использование многофакторной аутентификации для всех пользователей. | Необходимо использовать многофакторную аутентификацию и зашифрованные каналы для доступа к административной учетной записи. Группы реализации: группа реализации 2, группа реализации 3. | |
| 4.6 | Использование рабочих станций только для работы. | Необходимо убедиться, что администраторы используют выделенный компьютер для всех административных задач или задач, требующих административного доступа. Этот компьютер будет отделен от основной сети организации, и ему не будет разрешен доступ в Интернет. Группы реализации: группа реализации 3. | |
| 4.7 | Ограничение доступа к инструментам создания сценариев. | Необходимо ограничить доступ к инструментам создания сценариев (таким как Microsoft PowerShell и Python) только администраторам или пользователям-разработчикам, которым необходим доступ к этим возможностям. Группы реализации: группа реализации 2, группа реализации 3. | |
| 4.8 | Правильная настройка системы привилегий. | Необходимо настроить систему для создания записей в журнале и предупреждений, когда учетная запись добавляется или удаляется из любой привилегированной группы. Группы реализации: группа реализации 2, группа реализации 3. | |
| 4.9 | Ведения журнала неудачных попыток входа в административную учетную запись. | Необходимо настроить систему для создания записи в журнале и предупреждений о неудачных попытках входа в административную учетную запись. Группы реализации: группа реализации 2, группа реализации 3. | |

#### **Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers – Безопасная конфигурация оборудования и программного обеспечения на мобильных устройствах, ноутбуках, рабочих станциях и серверах.**

**Почему данный CIS важен?**

При поставке производителями мобильных устройств, ноутбуков и других видов электроники, используются базовые настройки системы, никак не ориентированные на защиту данных. Они по большей части ориентированы на простоту развёртывания. К сожалению, некоторые компании используют данные устройства без использования настроек повышенной безопасности. Разработка параметров конфигурации с хорошими свойствами безопасности - сложная задача, выходящая за рамки возможностей отдельных пользователей, требующая анализа сотен или тысяч вариантов видов настроек для того, чтобы сделать правильный выбор. Даже если надежная начальная конфигурация разработана и установлена производителем, то все равно, ее необходимо постоянно контролировать, чтобы избежать «разрушения» безопасности по мере обновления или исправления программного обеспечения. Ведь противном случае злоумышленники найдут возможности проникнуть вашу систему и украсть необходимые им данные.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 5: Безопасная конфигурация оборудования и ПО.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 5.1 | Поддержка стандартов конфигурации. | Необходимо поддерживать задокументированные стандарты конфигурации безопасности для всех авторизованных операционных систем и программного обеспечения. Группы реализации: группа реализации 1, группа реализации 2 и группа реализации 3. | |
| 5.2 | Использование защищенных и безопасных шаблонов. | Необходимо использовать безопасные образы или шаблоны для всех систем на предприятии в соответствии с утвержденными стандартами конфигурации организации. Любое развертывание новой системы следует создавать с помощью одного из этих образов или шаблонов, которые уже имеются у корпорации. Группы реализации: группа реализации 2, группа реализации 3. | |
| 5.3 | Хранение образов и шаблонов на надежных серверах. | Необходимо хранить главные образы и шаблоны на надежно настроенных серверах, проверенных с помощью инструментов мониторинга целостности для того, чтобы гарантировать, что возможность только санкционированных изменений образов. Группы реализации: группа реализации 2, группа реализации 3. | |
| 5.4 | Использование инструментов управления конфигурации системы. | Необходимо развернуть инструменты управления конфигурацией системы, которые будут автоматически применять и повторно развертывать параметры конфигурации в системах через регулярные запланированные интервалы. Группы реализации: группа реализации 2, группа реализации 3. | |
| 5.5 | Использование системы мониторинга конфигурации. | Необходимо использовать систему мониторинга конфигурации, совместимую с Security Content Automation Protocol (SCAP), чтобы проверить все элементы конфигурации безопасности, каталогизировать утвержденные исключения и предупредить о несанкционированных изменениях. Группы реализации: группа реализации 2, группа реализации 3. | |

#### **Control 6: Maintenance, Monitoring and Analysis of Audit Logs– Ведение, мониторинг и анализ журналов аудита**.

**Почему данный CIS важен?**

Недостатки в журналах безопасности и анализе позволяют злоумышленникам скрывать свое местоположение, вредоносное ПО и действия на машинах-жертвах. Даже если жертвы знают, что их системы были скомпрометированы, без защищенных и полных записей журналов они не видят деталей атаки и последующих действий, предпринятых злоумышленниками. Без надежных журналов аудита атака может оставаться незамеченной на неопределенное время, а нанесенный конкретный ущерб может быть необратимым.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 6: Ведение, мониторинг и анализ журналов аудита.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 6.1 | Использование синхронизированных источников времени. | Необходимо использовать минимум три синхронизированных источника времени, из которых все серверы и сетевые устройства регулярно получают информацию о времени, чтобы отметки времени в журналах были согласованными. Группы реализации: группа реализации 2 и группа реализации 3. | |
| 6.2 | Ведение журнала аудита. | Необходимо убедиться, что локальное ведение журнала включено во всех системах и сетевых устройствах. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 6.3 | Системное ведение журнала аудита. | Необходимо включить системное ведение журнала аудита, чтобы в последующем использовать подробную информацию, такую как источник события, дата, пользователь, отметка времени, адреса источника, адреса назначения и другие полезные элементы. Группы реализации: группа реализации 2, группа реализации 3. | |
| 6.4 | Уверенность в том, что в системах хватает места для хранения информации. | Необходимо убедиться, что во всех системах, в которых хранятся журналы, достаточно места для хранения создаваемых журналов. Группы реализации: группа реализации 2, группа реализации 3. | |
| 6.5 | Объединение журналов аудита в одну центральную систему. | Необходимо убедиться, что ведутся соответствующие журналы, объединенные в центральную систему управления журналами для анализа и просмотра. Группы реализации: группа реализации 2, группа реализации 3. | |
| 6.6 | Развертывание средств управления информацией. | Необходимо развернуть средства управления информацией и событиями безопасности (SIEM) или аналитические инструменты журналов. Группы реализации: группа реализации 2, группа реализации 3 | |
| 6.7 | Регулярный просмотр журналов аудита. | Необходимо регулярно просматривать журналы для выявления аномалий или аномальных событий. Группы реализации: группа реализации 2, группа реализации 3. | |
| 6.8 | Регулярная настройка SIEM-системы. | Необходимо регулярно настраивайте свою SIEM-систему, чтобы лучше определять события, требующие действий. Группы реализации: группа реализации 3. | |

#### **Control 7: Email and Web Browser Protections– Защита электронной почты и браузера**.

**Почему данный CIS важен?**

Веб-браузеры и почтовые клиенты являются очень распространенными способами атак на систему из-за их технической сложности, гибкости и прямого взаимодействия с пользователями, а также с другими системами и веб-сайтами. Контент может быть создан, чтобы побудить пользователей к действиям, которые значительно увеличивают риск и допускают внедрение вредоносного кода, потерю ценных данных и другие атаки. Поскольку эти приложения являются основным средством взаимодействия пользователей с ненадежными средами, они являются потенциальными целями как для эксплуатации кода, так и для социальной инженерии. Поэтому очень важно защищать электронную почту и браузеры.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 7: Защита электронной почты и браузера.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 7.1 | Использование полностью поддерживаемых веб-браузеров и почтовых клиентов. | Необходимо убедиться, что в организации разрешена работа только с полностью поддерживаемых веб-браузеров и почтовых клиентов, в идеале с использованием только последней версии браузеров и почтовых клиентов, предоставленных поставщиком. Группы реализации: группа реализации 1, группа реализации 2 и группа реализации 3. | |
| 7.2 | Удаление или отключения неавторизированных браузеров или почтовых клиентов. | Необходимо удалить или отключить любой неавторизированный веб-браузер или потовый клиент. Группы реализации: группа реализации 2, группа реализации 3. | |
| 7.3 | Разрешение работать только авторизованным сценариям. | Необходимо убедиться в том, что только авторизованные языки сценариев могут работать во всех веб-браузерах и почтовых клиентах. Группы реализации: группа реализации 2, группа реализации 3. | |
| 7.4 | Применение сетевых фильтров URL-адресов. | Необходимо применять сетевые фильтры URL-адресов, которые ограничивают возможность системы подключаться к веб-сайтам, не одобренным организацией. Эта фильтрация должна выполняться для каждой системы организации, независимо от того, находятся ли они физически на объектах организации или нет. Группы реализации: группа реализации 2, группа реализации 3. | |
| 7.5 | Подпись на серверы категоризации URL-адресов. | Необходимо подписаться на сервисы категоризации URL-адресов, чтобы убедиться, что они актуальны и соответствуют самым последним доступным определениям категорий веб-сайтов. Сайты без категорий по умолчанию блокируются. Группы реализации: группа реализации 2, группа реализации 3. | |
| 7.6 | Регистрация запросов URL-адресов. | Необходимо регистрировать все запросы URL-адресов от каждой системы организации, будь то это с компьютера или с мобильного устройства для того, чтобы идентифицировать потенциально вредоносную активность и помочь обработчикам инцидентов идентифицировать потенциально скомпрометированные системы. Группы реализации: группа реализации 2, группа реализации 3 | |
| 7.7 | Использование служб фильтрации DNS. | Необходимо использовать службы фильтрации системы доменных имен (DNS), чтобы заблокировать доступ к известным вредоносным доменам. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 7.8 | Внедрение политики и проверки подлинности сообщений, отчетности и соответствия. | Чтобы снизить вероятность поддельных или измененных электронных писем из допустимых доменов, необходимо внедрить политику и проверку подлинности сообщений, отчетности и соответствия (DMARC) на основе домена (DMARC), начиная с внедрения стандартов политики отправителя (SPF) и почтовых стандартов DomainKeys Identified Mail (DKIM). Группы реализации: группа реализации 2, группа реализации 3. | |
| 7.9 | Блокировка вложений электронной почты. | Необходимо заблокировать все вложения электронной почты, поступающие на шлюз электронной почты организации, если типы файлов не нужны для бизнеса организации. Группы пользователей: группы пользователей 2, группы пользователей 3. | |
| 7.10 | Использование песочницы для анализа и блокировки входящих сообщений. | Необходимо использовать песочницу для анализа и блокировки входящих сообщений электронной почты с вредоносным поведением. Группы пользователей: группы пользователей 3. | |

#### **Control 8: Malware Defenses– Защита от вредоносного ПО**.

**Почему данный CIS важен?**

Вредоносное программное обеспечение является неотъемлемым и самым опасным аспектом интернет-угроз, поскольку оно предназначено для атак на ваши системы, устройства и ваши данные. Он быстро движется, быстро меняется и поступает через любое количество точек, таких как устройства конечного пользователя, вложения электронной почты, веб-страницы, облачные службы, действия пользователя и съемные носители. Защита от вредоносного ПО должна работать в этой динамической среде за счет крупномасштабной автоматизации, быстрого обновления и интеграции с такими процессами, как реагирование на инциденты. Они также должны быть развернуты в нескольких возможных точках атаки, чтобы обнаруживать, останавливать движение или контролировать выполнение вредоносного программного обеспечения. Корпоративные пакеты безопасности конечных точек предоставляют административные функции для проверки того, что все средства защиты активны и актуальны в каждой управляемой системе.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 8: Защита от вредоносного ПО.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 8.1 | Использование централизованно управляемого антивирусного ПО. | Необходимо использовать централизованно управляемое антивирусное программное обеспечение для непрерывного мониторинга и защиты каждой из рабочих станций и серверов организации. Группы реализации: группа реализации 2 и группа реализации 3. | |
| 8.2 | Обновление модуля сканирования и баз данных сигнатур. | Необходимо убедиться, что антивирусное программное обеспечение организации регулярно обновляет свой модуль сканирования и базу данных сигнатур. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 8.3 | Включение функций защиты от эксплуатации. | Необходимо включить функции защиты от эксплуатации, предотвращение выполнения данных (DEP) и рандомизация разметки адресного пространства (ASLR), доступные в операционной системе, или развернуть соответствующие наборы инструментов, которые можно настроить для применения защиты к более широкому набору приложений и исполняемых файлов. Группы реализации: группа реализации 2, группа реализации 3. | |
| 8.4 | Настройка устройств для автоматического сканирования съемных носителей. | Необходимо настроить устройства так, чтобы они автоматически выполняли сканирование съемных носителей на наличие вредоносных программ при установке или подключении. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 8.5 | Настройка устройств для запрета автоматического запуска контента со съемных носителей. | Необходимо настроить устройства так, чтобы они не запускали контент со съемных носителей автоматически. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 8.6 | Отправка событий обнаружения вредосного ПО. | Необходимо отправлять все события обнаружения вредоносных программ в корпоративные средства администрирования защиты от вредоносных программ и на серверы журналов событий для анализа и предупреждения. Группы реализации: группа реализации1, группа реализации 2, группа реализации 3 | |
| 8.7 | Включение журнала DNS. | Необходимо включить ведение журнала запросов системы доменных имен (DNS), чтобы обнаруживать поиск имени хоста для известных вредоносных доменов. Группы реализации: группа реализации 2, группа реализации 3. | |
| 8.8 | Включения журнала аудита для командной строки. | Необходимо включить ведение журнала аудита командной строки для командных оболочек, таких как Microsoft PowerShell и Bash. Группы реализации: группа реализации 2, группа реализации 3. | |

#### **Control 9: Limitation and Control of Network Ports, Protocols and Services– Ограничение и контроль сетевых портов, протоколов и служб.**

**Почему данный CIS важен?**

Злоумышленники ищут удаленно доступные сетевые сервисы, уязвимые в эксплуатации. Распространенные примеры включают плохо настроенные веб-серверы, почтовые серверы, файловые службы и службы печати, а также DNS-серверы, установленные по умолчанию на различных типах устройств, часто без бизнес-необходимости в данной службе. Многие программные пакеты автоматически устанавливают службы и включают их как часть установки основного программного пакета, не информируя пользователя или администратора о том, что службы включены. Злоумышленники сканируют такие службы и пытаются использовать эти службы для взлома системы.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 9: Ограничение и контроль сетевых портов, протоколов и служб.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 9.1 | Объединение активных портов и т.д. с аппаратными активами в инвентаризации активов. | Необходимо связать активные порты, протоколы и службы с аппаратными активами в инвентаризации активов. Группы реализации: группа реализации 2 и группа реализации 3. | |
| 9.2 | Использование подтвержденных портов, протоколов и служб. | Необходимо убедиться, что в каждой системе работают только сетевые порты, протоколы и службы, прослушивающие систему с подтвержденными бизнес-потребностями. Группы реализации: группа реализации 2, группа реализации 3. | |
| 9.3 | Выполнение автоматического сканирование портов. | Необходимо выполнять автоматическое сканирование портов на регулярной основе для всех систем и предупреждайте, если в системе обнаруживаются неавторизованные порты. Группы реализации: группа реализации 2, группа реализации 3. | |
| 9.4 | Настройка межсетевых экранов и фильтрации портов. | Необходимо применять брандмауэры на основе хоста или инструментов фильтрации портов в конечных системах с явным разрешенным правилом отброса всего трафика кроме этих служб по умолчанию. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 9.5 | Блокировка или отбрасывание неавторизованного трафика. | Необходимо установить брандмауэры приложений перед всеми критически важными серверами для проверки и подтверждения трафика, идущего на сервер. Любой неавторизованный трафик следует блокировать и регистрировать. Группы реализации: группа реализации 3. | |

#### **Control 10: Data Recovery Capabilities– Возможность восстановления данных.**

**Почему данный CIS важен?**

Когда злоумышленники взламывают машины, они часто вносят значительные изменения в конфигурации и программное обеспечение. Иногда злоумышленники также вносят небольшие изменения в данные, хранящиеся на скомпрометированных машинах, потенциально ставя под угрозу эффективность организации из-за загрязненной информации. Поэтому после обнаружение взлома, очень важно восстановить свои данные в исходное состояние, чтобы в дальнейшем избежать проблем.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 10: Возможность восстановления данных.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 10.1 | Автоматическое регулярное копирование данных. | Необходимо обеспечить автоматическое регулярное резервное копирование всех системных данных. Группы реализации: группа реализации 1, группа реализации 2 и группа реализации 3. | |
| 10.2 | Резервное копирование всех ключевых систем организации. | Необходимо обеспечить резервное копирование всех ключевых систем организации, как целостной системы с помощью таких процессов, как создание образов, чтобы обеспечить быстрое восстановление всей системы. Группы реализации: группа реализации1, группа реализации 2, группа реализации 3. | |
| 10.3 | Проверка целостности данных на резервных копиях. | Необходимо регулярно проверять целостность данных на носителях резервных копий, выполняя процесс восстановления данных, чтобы убедиться, что резервная копия работает правильно. Группы реализации: группа реализации 2, группа реализации 3. | |
| 10.4 | Защита резервных копий. | Необходимо убедиться, что резервные копии должным образом защищены с помощью физической безопасности или шифрования при хранении, а также при их перемещении по сети. Это включает в себя удаленное резервное копирование и облачные сервисы. Группы реализации: группа реализации1, группа реализации 2, группа реализации 3. | |
| 10.5 | Создание автономного места назначения резервного копирования. | Необходимо убедиться, что у всех резервных копий есть хотя бы одно автономное (т. Е. Недоступное через сетевое соединение) место назначения резервного копирования. Группы реализации: группа реализации1, группа реализации 2, группа реализации 3. | |

#### **Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches– Безопасная конфигурация сетевых устройств, таких как межсетевые экраны, маршрутизаторы и коммутаторы.**

#### **Почему данный CIS важен?**

Конфигурации по умолчанию для устройств сетевой инфраструктуры, поставляемые производителями и торговыми посредниками, ориентированы на простоту развертывания и использования, а не на безопасность. Управление безопасными конфигурациями для сетевых устройств - это не разовое событие, а процесс, который включает регулярную переоценку не только элементов конфигурации, но и разрешенных потоков трафика. Злоумышленники пользуются тем, что сетевые устройства со временем становятся менее защищенными, поскольку пользователи требуют исключений для конкретных бизнес-нужд.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 11: Безопасная конфигурация сетевых устройств.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 11.1 | Поддержка задокументированных стандартов конфигурации. | Необходимо поддерживать задокументированные стандарты конфигурации безопасности для всех авторизованных сетевых устройств. Группы реализации: группа реализации 2 и группа реализации 3. | |
| 11.2 | Использование правил документации. | Все правила конфигурации, которые позволяют трафику проходить через сетевые устройства, должны быть задокументированы в системе управления конфигурацией с указанием конкретной бизнес-причины для каждого правила, имени конкретного лица, ответственного за эту бизнес-потребность, и ожидаемой продолжительности потребности. Группы реализации: группа реализации 2, группа реализации 3. | |
| 11.3 | Сравнение конфигураций устройств. | Необходимо сравнивать все конфигурации сетевых устройств с утвержденными конфигурациями безопасности, определенными для каждого используемого сетевого устройства, и предупредите при обнаружении любых отклонений. Группы реализации: группа реализации 2, группа реализации 3. | |
| 11.4 | Установка последних обновлений. | Необходимо установить последнюю стабильную версию любых обновлений, связанных с безопасностью, на все сетевые устройства. Группы реализации: группа реализации1, группа реализации 2, группа реализации 3. | |
| 11.5 | Управление сетевыми устройствами с помощью многофакторной аутентификации. | Необходимо управлять всеми сетевыми устройствами с помощью многофакторной аутентификации и зашифрованных сеансов. Группы реализации: группа реализации 2, группа реализации 3. | |
| 11.6 | Рабочая машина используется только для работы. | Необходимо убедиться, что сетевые инженеры используют выделенный компьютер для всех административных задач или задач, требующих повышенного доступа. Этот компьютер должен быть отделен от основной сети организации, и ему не должен быть разрешен доступ в Интернет. Группы реализации: группа реализации 2, группа реализации 3. | |
| 11.7 | Управление сетью инфраструктуры через отдельную выделенную сеть. | Управление сетевой инфраструктурой происходит через сетевые соединения, которые отделены от бизнес-использования этой сети, полагаясь на отдельные VLAN или, предпочтительно, на совершенно другие физические возможности подключения для сеансов управления для сетевых устройств. Группы реализации: группа реализации 2, группа реализации 3. | |

#### **Control 12: Boundary Defense** **– Защита периметра.**

#### **Почему данный CIS важен?**

Злоумышленники сосредотачиваются на использовании систем, к которым они могут подключиться через Интернет, включая не только системы DMZ, но также рабочие станции и портативные компьютеры, которые извлекают контент из Интернета через границы сети. Такие угрозы, как организованные преступные группировки и национальные государства, используют недостатки конфигурации и архитектуры, обнаруженные в системах периметра, сетевых устройствах и клиентских машинах с доступом в Интернет, для получения первоначального доступа в организацию. Затем, имея базу операций на этих машинах, злоумышленники часто углубляются в границу, чтобы украсть или изменить информацию, или настроить постоянное присутствие для последующих атак на внутренние хосты. Поэтому очень ажно защищать границы сети, а также фильтровать как входящий, так и исходящий трафик.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 12: Защита периметра.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 12.1 | Ведение инвентаризации границ сети. | Необходимо поддерживать актуальную инвентаризацию всех границ сети организации. Группы реализации: группа реализации 1, группа реализации 2 и группа реализации 3. | |
| 12.2 | Выполнение регулярных сканирований извне. | Необходимо выполнять регулярное сканирование извне каждой доверенной границы сети для обнаружения любых неавторизованных подключений, доступных через границу. Группы реализации: группа реализации 2, группа реализации 3. | |
| 12.3 | Запрет обмена данных с ненадежными IP-адресами. | Необходимо запретить обмен данными с известными вредоносными или неиспользуемыми IP-адресами в Интернете и ограничьте доступ только к надежным и необходимым диапазонам IP-адресов на каждой границе сети организации. Группы реализации: группа реализации 2, группа реализации 3. | |
| 12.4 | Запрет обмена данных через неавторизованные порты TCP и UDP. | Необходимо запретить обмен данными через неавторизованные порты TCP или UDP, или трафик приложений, чтобы гарантировать, что только авторизованные протоколы могут пересекать граница сети внутри или вне сети на каждой из границ сети организации. Группы реализации: группа реализации1, группа реализации 2, группа реализации 3. | |
| 12.5 | Настройка мониторинга системы. | Необходимо настроить системы мониторинга для записи сетевых пакетов, проходящих через границу на каждой границе сети организации. Группы реализации: группа реализации 2, группа реализации 3. | |
| 12.6 | Развёртывание сетевых датчиков систем обнаружения вторжений (IDS). | Необходимо провести развёртывание сетевых датчиков систем обнаружения вторжений (IDS) для поиска необычных механизмов атаки и обнаружения компрометации этих систем на каждой границе сети организации. Группы реализации: группа реализации 2, группа реализации 3. | |
| 12.7 | Развёртывание сетевых систем предотвращения вторжений (IPS) | Необходимо развернуть сетевые системы предотвращения вторжений (IPS) для блокировки вредоносного сетевого трафика на каждой границе сети организации. Группы реализации: группа реализации 3. | |
| 12.8 | Включение NetFlow | Необходимо включить сбор NetFlow и запись данных на всех сетевых граничных устройствах. Группы реализации: группа реализации 2, группа реализации 3. | |
| 12.9 | Фильтрация неавторизованных подключений. | Необходимо убедиться, что весь сетевой трафик в Интернет или из него, проходит через проверенный прокси-сервер уровня приложений, который настроен для фильтрации неавторизованных подключений. Группы реализации: группа реализации 3. | |
| 12.10 | Расшифровка зашифрованного сетевого трафика. | Необходимо расшифровать весь зашифрованный сетевой трафик на граничном прокси перед анализом содержимого. Группы реализации: группа реализации 3. | |
| 12.11 | Требование удаленного доступа к сети. | Необходимо требовать удаленный доступ к сети организации для шифрования передаваемых данных и использования многофакторной аутентификации. Группы реализации: группа реализации 2, группа реализации 3. | |
| 12.12 | Сканирование корпоративных устройств. | Сканируйте все корпоративные устройства с удаленным входом в сеть организации перед доступом к сети, чтобы убедиться, что все политики применяются верно. Группы реализации: группа реализации 3. | |

#### **Control 13: Data Protection– Защита данных.**

#### **Почему данный CIS важен?**

Данные хранятся на разных носителях информации. Защита этих данных лучше всего достигается за счет применения комбинации методов шифрования, защиты целостности и предотвращения потери данных. По мере того, как организации продолжают двигаться к облачным вычислениям и мобильному доступу, важно принимать надлежащие меры для ограничения утечки данных и отчетности о них, а также для смягчения последствий компрометации данных.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 13: Защита данных.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 13.1 | Ведение перечня конфиденциальной информации. | Необходимо вести инвентаризацию всей конфиденциальной информации, хранящейся, обрабатываемой или передаваемой системами организации, включая те, которые расположены на территории предприятия или у удаленного поставщика услуг. Группы реализации: группа реализации 1, группа реализации 2 и группа реализации 3. | |
| 13.2 | Удаление из сети ненужных систем. | Необходимо удалить из сети системы, к которым организация не обращается регулярно. Эти системы должны использоваться только как автономные системы (отключенные от сети) бизнес-подразделением, которому необходимо время от времени использовать систему .Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 13.3 | Развертывание инструмента, отслеживающего несанкционированную передачу данных. | Необходимо развернуть автоматизированный инструмент на периметрах сети, который отслеживает несанкционированную передачу конфиденциальной информации и блокирует такую передачу, одновременно предупреждая специалистов по информационной безопасности. Группы реализации: группа реализации 3. | |
| 13.4 | Разрешение на доступ только к авторизированных средствам. | Необходимо разрешить доступ только к авторизованному облачному хранилищу или поставщикам электронной почты. Группы реализации: группа реализации 2, группа реализации 3. | |
| 13.5 | Мониторинг и обнаружение любого несанкционированного использования сети. | Необходимо отслеживать весь трафик, покидающий организацию, и обнаруживать любое несанкционированное использование шифрования. Группы реализации: группа реализации 3. | |
| 13.6 | Использование утвержденных криптографических механизмов. | Необходимо использовать утвержденные криптографические механизмы для защиты корпоративных данных, хранящихся на всех мобильных устройствах. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 13.7 | Управление USB-устройствами. | Если требуются USB-устройства хранения данных, следует использовать корпоративное программное обеспечение, которое может настраивать системы для разрешения использования определенных устройств. Следует вести перечень таких устройств. Группы реализации: группа организации 2 группа реализации 3. | |
| 13.8 | Управление внешними носителями. | Необходимо настроить системы так, чтобы они не записывали данные на внешние съемные носители, если нет бизнес-необходимости в поддержке таких устройств. Группы реализации:, группа реализации 3. | |
| 13.9 | Шифрование данных на USB-носителях. | Если требуются USB-устройства хранения данных, все данные, хранящиеся на таких устройствах, должны быть зашифрованы вовремя хранения. Группы реализации: группа реализации 3. | |

#### **Control 14: Controlled Access Based on the Need to Know– Контроль доступа к данным.**

#### **Почему данный CIS важен?**

Шифрование данных обеспечивает определенный уровень уверенности в том, что даже в случае компрометации данных доступ к открытому тексту без значительных затрат на расшифровку невозможен. Тем не менее, необходимо иметь средства управления шифрованием для того, чтобы в первую очередь снизить угрозу кражи данных. Передвижение данных через границы сети как в электронном, так и в физическом смысле должно тщательно контролироваться, чтобы свести к минимуму его уязвимость для злоумышленников. Потеря контроля над защищенными или конфиденциальными данными организациями - серьезная угроза бизнес-операциям и потенциальная угроза национальной безопасности.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 14: Контроль доступа к данным.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 14.1 | Сегментирование сети. | Сегментация сети на основе уровня классификации конфиденциальности информации, хранящейся на серверах. Группы реализации: группа реализации 2 и группа реализации 3. | |
| 14.2 | Включение фильтрации брандмауэра между VLAN. | Необходимо включить фильтрацию межсетевого экрана между сетями VLAN, чтобы только авторизованные системы могли связываться с другими системами, необходимыми для выполнения их конкретных обязанностей. Группы реализации: группа реализации 2, группа реализации 3. | |
| 14.3 | Отключение рабочих станций. | Необходимо отключить все рабочие станции обмена данных, чтобы ограничить способность злоумышленника перемещаться и компрометировать соседние системы с помощью частных VLAN или микросегментации. Группы реализации: группа реализации 3. | |
| 14.4 | Шифрование информации. | Шифрование конфиденциальной информации при ее передаче. Группы реализации: группа реализации 2, группа реализации 3. | |
| 14.5 | Использование активного инструмента обнаружения данных. | Необходимо использовать активный инструмент обнаружения данных, чтобы идентифицировать всю конфиденциальную информацию, хранящуюся, обрабатываемую или передаваемую организацией. Группы реализации: группа реализации 3. | |
| 14.6 | Использование списков доступа к конфиденциальной информации. | Необходимо защищать всю информацию, хранящуюся в системах, с помощью списков управления доступом файловой системы, общего сетевого ресурса, заявок, приложений или баз данных. Эти средства контроля будут обеспечивать соблюдение принципа, согласно которому только уполномоченные лица должны иметь доступ к информации, исходя из их потребности в доступе к информации в рамках своих обязанностей. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 14.7 | Использование автоматизированного инструмента для предотвращения потери данных. | Необходимо использовать автоматизированный инструмент, такой как предотвращение потери данных на основе хоста, для обеспечения контроля доступа к данным, даже когда данные копируются из системы. Группы реализации: группа реализации 3. | |
| 14.8 | Шифрование информации. | Необходимо зашифровать всю конфиденциальную информацию при хранении с помощью инструмента, который требует вторичного механизма аутентификации, не интегрированного в операционную систему. Группы реализации:, группа реализации 3. | |
| 14.9 | Ведение журнала аудита для доступа к конфиденциальным данным. | Необходимо обеспечить подробное ведение журнала аудита для доступа к конфиденциальным данным или изменения их (с использованием таких инструментов, как мониторинг целостности файлов или мониторинг информации и событий безопасности). Группы реализации: группа реализации 3. | |

#### **Control 15: Wireless Access Control– Контроль беспроводного доступа.**

#### **Почему данный CIS важен?**

Крупные кражи данных были проведены злоумышленниками, через беспроводной доступ к организациям из-за пределов физического здания, минуя периметры безопасности организации, просто подключившись по беспроводной сети к точкам доступа внутри организации. Беспроводные клиенты работников организации регулярно заражаются через использование интернета в общественных местах. Такие эксплуатируемые системы затем используются как лазейки при повторном подключении к сети целевой организации.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 15: Контроль доступа к данным.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 15.1 | Ведение учета авторизованных точек беспроводной сети. | Необходимо вести учет авторизованных точек беспроводного доступа, подключенных к проводной сети. Группы реализации: группа реализации 2 и группа реализации 3. | |
| 15.2 | Настройка инструментов сканирования уязвимостей сети. | Необходимо настроить инструменты сканирования уязвимостей сети для обнаружения и предупреждения о неавторизованных точках беспроводного доступа, подключенных к проводной сети. Группы реализации: группа реализации 2, группа реализации 3. | |
| 15.3 | Использование WIDS. | Необходимо использовать беспроводную систему обнаружения вторжений (WIDS) для обнаружения и оповещения о неавторизованных точках беспроводного доступа, подключенных к сети. Группы реализации: группа реализации 2, группа реализации 3. | |
| 15.4 | Отключение беспроводного доступа на устройствах, если не требуется. | Необходимо отключить беспроводной доступ на устройствах, не предназначенных для использования в бизнесе. Группы реализации: группа реализации 3. | |
| 15.5 | Ограничение беспроводного доступа на клиентских устройствах. | Необходимо настроить беспроводной доступ на клиентских машинах, которые действительно имеют важное значение для беспроводного бизнеса, чтобы разрешить доступ только к авторизованным беспроводным сетям и ограничить доступ к другим беспроводным сетям. Группы реализации: группа реализации 3. | |
| 15.6 | Отключение возможностей одноранговой сети. | Необходимо отключить возможности одноранговой (ad hoc) беспроводной сети на беспроводных клиентах. Группы реализации: группа реализации 2, группа реализации 3. | |
| 15.7 | Использование расширенного стандарта шифрования. | Необходимо использовать расширенный стандарт шифрования (AES) для шифрования передаваемых беспроводных данных. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 15.8 | Использования протоколов многофакторной аутентификации. | Необходимо убедиться, что в беспроводных сетях используются протоколы аутентификации, такие как Extensible Authentication Protocol-Transport Layer Security (EAP / TLS), которые требует взаимной многофакторной аутентификации. Группы реализации: группа реализации 3. | |
| 15.9 | Отключение беспроводного периферийного доступа к устройствам. | Необходимо отключить беспроводной периферийный доступ к устройствам [например, Bluetooth и связь ближнего радиуса действия (NFC)], если такой доступ не требуется для деловых целей. Группы реализации: группа реализации 2, группа реализации 3. | |
| 15.10 | Создание отдельной беспроводной сети для ненадежных устройств. | Необходимо создать отдельную беспроводную сеть для личных или ненадежных устройств. Доступ предприятия из этой сети следует рассматривать как ненадежный и соответствующим образом фильтровать и проверять. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |

#### **Control 16: Account Monitoring and Control– Мониторинг и контроль учетных записей.**

#### **Почему данный CIS важен?**

Злоумышленники часто обнаруживают и используют неактивные учетные записи пользователей, чтобы выдать себя за владельцев этих аккаунтов, тем самым затрудняя свое обнаружение в сети. Учетные записи подрядчиков и сотрудников, которые были уволены, и учетные записи, ранее созданные для тестирования Red Team (но не удаленные впоследствии), часто используются таким образом. Кроме того, некоторые злонамеренные инсайдеры или бывшие сотрудники, получившие доступ к учетным записям, оставленным в системе, спустя много времени после истечения срока действия контракта, сохраняют свой доступ к вычислительной системе организации и конфиденциальным данным для несанкционированных, а иногда и злонамеренных целей.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 16: мониторинг и контроль учетных записей.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 16.1 | Ведение инвентаризации аккаунтов системы. | Необходимо вести инвентаризацию каждого аккаунта из системы аутентификации организации, в том числе расположенные на территории или у удаленного поставщика услуг. Группы реализации: группа реализации 2 и группа реализации 3. | |
| 16.2 | Настройка доступа учетных записей к системе. | Необходимо настроить доступ для всех учетных записей через как можно меньше централизованных точек аутентификации, включая сетевые, безопасные и облачные системы. Группы реализации: группа реализации 2, группа реализации 3. | |
| 16.3 | Требование многофакторной аутентификации. | Необходимо требовать многофакторную аутентификацию для всех учетных записей пользователей во всех системах, независимо от того, управляются ли они на месте или сторонним поставщиком. Группы реализации: группа реализации 2, группа реализации 3. | |
| 16.4 | Шифрование и хеширование учетных данных. | Необходимо шифровать или хешировать все учетные данные аутентификации при сохранении. Группы реализации: группа реализации 2, группа пользователей 3. | |
| 16.5 | Передача данных по зашифрованным каналам. | Необходимо убедиться, что все имена пользователей и учетные данные для аутентификации передаются по сетям с использованием зашифрованных каналов. Группы реализации: группа реализации 2, группа реализации 3. | |
| 16.6 | Ведение инвентаризации учетных записей. | Необходимо вести инвентаризацию всех учетных записей, организованных системой аутентификации. Группы реализации: группа реализации 2, группа реализации 3. | |
| 16.7 | Отключение ненужных учетныхзаписей. | Необходимо установить и соблюдать автоматизированный процесс отмены доступа к системе путем отключения учетных записей сразу после прекращения или изменения обязанностей сотрудника или подрядчика. Отключение учетных записей вместо удаления их позволяет сохранить контрольные журналы. Группы реализации: группа реализации 2, группа реализации 3. | |
| 16.8 | Отключение учетных записей, несвязанных с бизнесом. | Необходимо отключить любую учетную запись, которая не может быть связана с бизнес-процессом или владельцем бизнеса. Группы реализации: группа реализации 1, группа аутентификации 2, группа реализации 3. | |
| 16.9 | Отключение неактивных учетных записей. | Необходимо автоматически отключать неактивные учетные записи после определенного периода бездействия. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 16.10 | Наличие срока действия учетных записей. | Необходимо убедиться, что у всех учетных записей есть срок действия, который отслеживается и применяется. Группы реализации: группа реализации 2, группа реализации 3. | |
| 16.11 | Блокировка сеансов учетных записей. | Автоматически блокировать сеансы рабочей станции после стандартного периода бездействия. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 16.12 | Отслеживание попыток доступа к деактивированным учетным записям. | Необходимо отслеживать попытки доступа к деактивированным учетным записям с помощью журнала аудита. Группы реализации: группа реализации 2, группа реализации 3. | |
| 16.13 | Отслеживание поведения входа в систему. | Необходимо оповещать, когда пользователи отклоняются от обычного поведения входа в систему, например, время суток, расположение рабочей станции и продолжительность сеанса. Группы реализации: группа реализации 3. | |

#### **Control 17: Implement a Security Awareness and Training Program** **– Контроль осведомленности уровня персонала.**

#### **Почему данный CIS важен?**

Неправильно думать о киберзащите в первую очередь, как о технической проблеме, ведь действия людей также играют решающую роль в успехе или неудаче информационной защиты предприятия. Люди выполняют важные функции на каждом этапе проектирования, внедрения, эксплуатации, использования и контроля системы. Например: системные разработчики и программисты (которые могут не понимать возможности устранения уязвимостей, являющихся первопричиной уязвимостей, на ранних этапах жизненного цикла системы); Специалисты по ИТ-операциям (которые могут не осознавать последствия для безопасности артефактов и журналов ИТ); конечные пользователи (которые могут быть уязвимы для схем социальной инженерии, таких как фишинг); аналитики безопасности (которые изо всех сил стараются не отставать от всплеска новой информации); а также руководители и владельцы систем (которые пытаются количественно оценить роль, которую кибербезопасность играет в общем операционном риске / риске миссии, все они являются основной целью злоумышленников для кражи конфиденциальной информации.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 17: контроль осведомленности уровня персонала.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 17.1 | Проведения анализа навыков сотрудников. | Необходимо проводить анализ пробелов в навыках сотрудников, чтобы понять, какие правила сотрудники не соблюдают, используя эту информацию для построения базовой дорожной карты образования. Группы реализации: группа реализации 2 и группа реализации 3. | |
| 17.2 | Проведение обучений для устранения пробелов. | Необходимо проведение обучение для устранения выявленного пробела в навыках, который положительно повлияет на поведение сотрудников в области безопасности. Группы реализации: группа реализации 2, группа реализации 3. | |
| 17.3 | Создание информационной программы по обеспечению безопасности. | Необходимо создать программу повышения осведомленности о безопасности, которую должны регулярно выполнять все сотрудники, чтобы убедиться, что они понимают и демонстрируют необходимое поведение и навыки, помогающие обеспечить безопасность организации. Информационная программа организации по обеспечению безопасности должна передаваться непрерывно и увлекательно. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 17.4 | Проверка обновлений программы. | Необходимо убедиться, что программа осведомленности о безопасности организации часто обновляется (не реже одного раза в год) с учетом новых технологий, угроз, стандартов и бизнес-требований. Группы реализации: группа реализации 2, группа пользователей 3. | |
| 17.5 | Обучение сотрудников насчет важности безопасной аутентификации. | Необходимо обучить сотрудников важности включения и использования безопасной аутентификации. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 17.6 | Обучение сотрудников выявлению социальных атак. | Необходимо обучить персонал тому, как выявлять различные формы атак социальной инженерии, такие как фишинг, мошенничество по телефону и звонки с имитацией лица. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 17.7 | Обучение сотрудников работе с конфиденциальной информацией. | Необходимо обучить сотрудников тому, как выявлять и правильно хранить, передавать, архивировать и уничтожать конфиденциальную информацию. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 17.8 | Обучение сотрудников причинам непреднамеренного раскрытия данных. | Необходимо обучить сотрудников знать причины непреднамеренного раскрытия данных, например, потерю мобильных устройств или отправку электронной почты не тому человеку из-за автозаполнение по электронной почте. Группы реализации: группа реализации 1, группа аутентификации 2, группа реализации 3. | |
| 17.9 | Обучение сотрудников определять признаки инцидента. | Необходимо обучить сотрудников определять наиболее распространенные признаки инцидента и сообщать о таком инциденте. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |

#### **Control 18: Application Software Security– Безопасность прикладного программного обеспечения.**

#### **Почему данный CIS важен?**

Атаки злоумышленников часто используют уязвимости, обнаруженные в веб-приложениях. Уязвимости могут присутствовать по многим причинам, включая ошибки кодирования, логические ошибки, неполные требования и невозможность тестирования необычных или неожиданных условий. Примеры конкретных ошибок включают: неспособность проверить размер пользовательского ввода; невозможность отфильтровать ненужные, но потенциально вредоносные последовательности символов из входных потоков; сбой инициализации и очистки переменных; и плохое управление памятью, позволяющее недостаткам в одной части программного обеспечения влиять на несвязанные (и более важные для безопасности) части. Поэтому очень важно обеспечивать безопасность прикладного ПО.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 18: безопасность прикладного программного обеспечения.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 18.1 | Установка методов безопасного кодирования. | Необходимо установить методы безопасного кодирования, соответствующие используемому языку программирования и среде разработки. Группы реализации: группа реализации 2 и группа реализации 3. | |
| 18.2 | Проверка выполнения и документирования ошибок. | Для программного обеспечения собственной разработки важно убедиться, что выполняется и задокументирована явная проверка ошибок для всех входных данных, включая размер, тип данных и допустимые диапазоны или форматы. Группы реализации: группа реализации 2, группа реализации 3. | |
| 18.3 | Проверка версии ПО. | Необходимо убедиться, что версия всего программного обеспечения, приобретенного за пределами вашей организации, по-прежнему поддерживается разработчиком или имеет соответствующую защиту на основе рекомендаций разработчика по безопасности. Группы реализации: группа реализации 2, группа реализации 3. | |
| 18.4 | Использование современных сторонних компонентов для ПО. | Необходимо использовать только современные и проверенные сторонние компоненты для программного обеспечения, разработанного организацией. Группы реализации: группа пользователей 3. | |
| 18.5 | Использование стандартизированных алгоритмов шифрования. | Необходимо использовать только стандартизированные, принятые в настоящее время и тщательно проверенные алгоритмы шифровании. Группы реализации: группа реализации 2, группа реализации 3. | |
| 18.6 | Проверка знаний. | Необходимо убедиться, что весь персонал, занимающийся разработкой программного обеспечения, прошел обучение по написанию безопасного кода для своей конкретной среды разработки и обязанностей. Группы реализации: группа реализации 2, группа реализации 3. | |
| 18.7 | Применение инструментов статического и динамического анализа. | Необходимо применять инструменты статического и динамического анализа, чтобы убедиться, что методы безопасного кодирования соблюдаются для внутреннего программного обеспечения. Группы реализации: группа реализации 2, группа реализации 3. | |
| 18.8 | Получение отчетов об уязвимостях ПО. | Необходимо установить процесс приема и обработки отчетов об уязвимостях программного обеспечения, в том числе предоставление средств внешним организациям для связи с вашей группой безопасности. Группы реализации: группа аутентификации 2, группа реализации 3. | |
| 18.9 | Поддержка отдельных сред для производственных и непроизводственных систем. | Необходимо поддерживать отдельные среды для производственных и непроизводственных систем. Разработчики не должны иметь неконтролируемый доступ к производственной среде. Группы реализации: группа реализации 2, группа реализации 3. | |
| 18.10 | Защита веб-приложений. | Необходимо защитить веб-приложения, развернув брандмауэры веб-приложений (WAF), которые проверяют весь трафик, поступающий в веб-приложение, на предмет распространенных атак веб-приложений. Для приложений, которые не являются веб-приложениями, следует развернуть специальные брандмауэры приложений, если такие инструменты доступны для данного типа приложения. Группы реализации: группа реализации 2, группа реализации 3. | |
| 18.11 | Использование стандартных шаблонов конфигурации усиления защиты. | Для приложений, которые полагаются на базу данных, необходимо использовать стандартные шаблоны конфигурации усиления защиты. Все системы, которые являются частью критических бизнес-процессов, также должны быть протестированы. Группы реализации: группа реализации 2, группа реализации 3. | |

#### **Control 19: Incident Response and Management– Реагирования на инциденты и управление.**

#### **Почему данный CIS важен?**

Киберинциденты теперь просто часть нашего образа жизни. Даже крупные, хорошо финансируемые и технически продвинутые предприятия изо всех сил пытаются справиться с частотой и сложностью атак. Правильный вопрос, задаваемый успешной кибератаке на предприятие это не «если», а «когда» она произойдет. Когда происходит инцидент, уже слишком поздно разрабатывать правильные процедуры, отчеты, сбор данных, ответственность руководства, юридические протоколы и коммуникационную стратегию, которые позволят предприятию успешно понять, управлять и восстанавливаться. Без плана реагирования на инциденты организация может не обнаружить атаку, или, если атака будет обнаружена, организация может не следовать надлежащим процедурам для сдерживания ущерба, устранения присутствия злоумышленника и восстановления безопасным способом. Таким образом, злоумышленник может оказать гораздо большее влияние, нанеся больший ущерб, заразив большее количество систем и потенциально похитив более конфиденциальные данные, чем это было бы возможно при наличии эффективного плана реагирования на инциденты.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 19: реагирование на инциденты и управление.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 19.1 | Наличие письменного плана. | Необходимо убедиться, что есть письменные планы реагирования на инциденты, которые определяют роли персонала, а также этапы обработки / управления инцидентами. Группы реализации: группа реализации 1, группа реализации 2 и группа реализации 3. | |
| 19.2 | Назначение должностей и обязанностей в случае происхождения инцидента. | Необходимо назначить должности и обязанности по обработке компьютерных и сетевых инцидентов конкретным лицам, а также обеспечить отслеживание и документирование инцидента посредством разрешения. Группы реализации: группа реализации 2, группа реализации 3. | |
| 19.3 | Назначение управленческого персонала и создание резервных копий . | Необходимо назначить управленческий персонал, а также создать резервных копий, которые будут поддерживать процесс обработки инцидентов, выполняя ключевые роли при принятии решений. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 19.4 | Разработка общеорганизационных стандартов. | Важно разработать общеорганизационные стандарты в отношении времени, необходимого системным администраторам и другим членам персонала для сообщения об аномальных событиях группе обработки инцидентов, механизмов такого сообщения и типа информации, которая должна быть включена в уведомление об инциденте. Группы реализации: группа пользователей 2, группа пользователей 3. | |
| 19.5 | Сбор и хранения информации о сторонних контактных данных. | Необходимо собрать и хранить информацию о сторонних контактных данных, которые будут использоваться для сообщения об инцидентах безопасности, таких как правоохранительные органы, соответствующие государственные ведомства, поставщики и партнеры Центра обмена и анализа информации (ISAC). Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 19.6 | Публикация информации для сотрудников. | Необходимо публиковать информацию для всех сотрудников, касающуюся сообщения о компьютерных аномалиях и инцидентах группе обработки инцидентов. Такую информацию следует включать в обычные мероприятия по повышению осведомленности сотрудников. Группы реализации: группа реализации 1, группа реализации 2, группа реализации 3. | |
| 19.7 | Проведение стандартных упражнений и сценариев реагирования на инциденты. | Необходимо планировать и проводить стандартные упражнения и сценарии реагирования на инциденты для сотрудников, участвующих в реагировании на инциденты, чтобы поддерживать осведомленность и комфорт при реагировании на реальные угрозы. В ходе упражнений следует проверить каналы связи, принятие решений и технические возможности лиц, ответственных за инциденты, с использованием доступных им инструментов и данных. Группы реализации: группа реализации 2, группа реализации 3. | |
| 19.8 | Создание схемы расстановки приоритетов. | Необходимо создать схему оценки инцидентов и расстановки приоритетов на основе известного или потенциального воздействия на вашу организацию. Используйте оценку, чтобы определить частоту обновления статуса и процедуры эскалации. Группы реализации:, группа реализации 3. | |

#### **Control 20: Penetration Tests and Red Team Exercises– Тестирование на проникновение/Red Team.**

#### **Почему данный CIS важен?**

Злоумышленники часто используют дыры между хорошими защитными планами и намерениями, и их реализацией или обслуживанием. Примеры: временной интервал между объявлением об уязвимости, доступностью исправления поставщика и фактической установкой на каждой машине. Другие примеры включают: политику с благими намерениями, не имеющую механизма принуждения (особенно те, которые предназначены для ограничения рискованных действий человека); невозможность применить правильные конфигурации к машинам, которые включаются и выключаются из сети; и непонимание взаимодействия между несколькими защитными инструментами или с обычными операциями системы, которые имеют последствия для безопасности. В учениях Red Team используется комплексный подход ко всему спектру организационных политик, процессов и средств защиты, чтобы повысить организационную готовность, улучшить подготовку защитников и проверить текущие уровни эффективности.

|  |  |  |  |
| --- | --- | --- | --- |
| **CIS Control 20: тестирование на проникновение/ Red Team.** | | | **Применение** |
| **Под-тип** | **Описание под-типа** | **Описание контроля и группы реализации, где они используются.** | |
| 20.1 | Разработка программы тестов. | Необходимо разработать программу тестов на проникновение, которая включает в себя полный спектр смешанных атак, таких как атаки на беспроводные сети, атаки на основе клиентов и веб-приложения. Группы реализации: группа реализации 2 и группа реализации 3. | |
| 20.2 | Проведение внешних и внутренних тестов на проникновение. | Необходимо регулярно проводить внешние и внутренние тесты на проникновение для выявления уязвимостей и векторов атак, которые можно использовать для успешного использования корпоративных систем. Группы реализации: группа реализации 2, группа реализации 3. | |
| 20.3 | Выполнение тестов Red Team. | Необходимо выполнять периодические упражнения Red Team, чтобы проверить готовность организации выявлять и пресекать атаки или быстро и эффективно реагировать на угрозы. Группы реализации: группа реализации 3. | |
| 20.4 | Включение тестов на наличие незащищенной системной информации. | Необходимо включить тесты на наличие незащищенной системной информации и артефактов, которые могут быть полезны злоумышленникам, включая сетевые диаграммы, файлы конфигурации, старые отчеты о тестах на проникновение, электронные письма или документы, содержащие пароли или другую информацию, критически важную для работы системы. Группы реализации: группа пользователей 2, группа пользователей 3. | |
| 20.5 | Создание испытательного стенда. | Необходимо создать испытательный стенд, который имитирует производственную среду для определенных тестов на проникновение и атак Red Team на элементы, которые обычно не тестируются в производственной среде, например, атаки на системы диспетчерского управления, сбора данных и другие системы управления. Группы реализации: группа реализации 2, группа реализации 3. | |
| 20.6 | Использование инструментов сканирования уязвимостей. | Необходимо использовать инструменты сканирования уязвимостей и тестирования на проникновение вирусов в систему. Группы реализации: группа реализации 2, группа реализации 3. | |
| 20.7 | Документация результатов тестирования Red Team. | По возможности необходимо убедиться, что результаты Red Team задокументированы с использованием открытых машиночитаемых стандартов (например, SCAP). Важно разработать метод подсчета очков для определения результатов упражнений Red Team, чтобы результаты можно было сравнивать с течением времени. Группы реализации: группа реализации 3. | |
| 20.8 | Контроль учетных записей. | Любые пользовательские или системные учетные записи, используемые для выполнения тестирования на проникновение, должны контролироваться. Группы реализации: группа реализации 2, группа реализации 3. | |

**Вывод:**

В **CIS Controls 7** были внесены некоторые изменения по сравнению с прошлыми частями. В частности, был изменен приоритет некоторых рекомендаций (рекомендации в руководстве отсортированы по степени важности) для того, чтобы лучше отражать текущую ситуацию в мире киберугроз. Помимо этого, все рекомендации в **CIS Controls V7** были разделены на 3 категории: **базовые**, **основополагающие** и **организационные**.

В категории «**Базовые**» (CIS Controls 1-6) содержатся рекомендации по ключевым элементам управления, которые должны быть реализованы в каждой организации для обеспечения необходимой киберзащиты.

В категорию «**Основополагающих**» (CIS Controls 7-16) попали меры по кибербезопасности, обеспечивающие четкие преимущества в области защиты от киберугроз для различных организаций.

Категория «**Организационные**» (CIS Controls 17-20) ориентирована в основном на людей и процессы, связанные с кибербезопасностью. В ней описаны такие меры по обеспечению безопасности, как правильная работа с персоналом и рекомендации по реагированию на инциденты.

Рекомендации **CIS Controls** обеспечивают четкое, приоритетное руководство, помогающее организациям решать самые распространенные проблемы в сфере киберугроз. Эти рекомендации позволяют составить четкие и приоритетные руководства для решения задач по обеспечению информационной безопасности организации и могут быть использованы как основа политик информационной безопасности.

Авторы **CIS Controls 7** актуализировали рекомендации в соответствии с современными киберугрозами и приблизили их к сегодняшним реалиям. Новая версия руководства более структурирована: все рекомендации в ней разделены на три основные категории, что позволит специалистам по кибербезопасности при внедрении этих практик действовать от простого к сложному. Данный документ содержит ценные рекомендации по защите информации в современном мире, что безусловно поможет корпорациям в сфере IT обеспечить комплексную защиту конфиденциальной информации от кибератак.