Научная статья
Original article
УДК 004.424

УПРАВЛЕНИЕ РИСКАМИ КИБЕРБЕЗОПАСНОСТИ

CYBER SECURITY RISK MANAGEMENT

Казарян Каторина Камоевна студент специалитета, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kazaryan_katorina@mail.ru

Kazaryan Katorina Kamoevna specialty student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kazaryan_katorina@mail.ru

Аннотация: Управление рисками кибербезопасности - это стратегический подход к приоритизации угроз. Организации внедряют управление рисками кибербезопасности, чтобы обеспечить своевременное устранение наиболее серьезных угроз. Этот подход помогает выявлять, анализировать, оценивать и устранять угрозы на основе потенциального воздействия каждой угрозы.

Abstract: Cybersecurity risk management is a strategic approach to prioritizing threats. Organizations are implementing cybersecurity risk management to ensure that the most critical threats are addressed in a timely manner. This approach helps you identify, analyze, assess and remediate threats based on the potential impact of each threat.

Ключевые слова: кибератака, киберугроза, бот, несанкционированный доступ

Keywords: cyber attack, cyber threat, bot, unauthorized access

Стратегия управления рисками признает, что организации не могут полностью устранить все уязвимости системы или заблокировать все кибератаки . Создание инициативы по управлению рисками кибербезопасности помогает организациям в первую очередь обращать внимание на наиболее критические недостатки, тенденции угроз и атаки.

Вообще говоря, процесс управления рисками кибербезопасности включает четыре этапа:

- **Выявление риска** - оценка среды организации для выявления текущих или потенциальных рисков, которые могут повлиять на бизнес-операции.
- **Оценка риска** - анализ выявленных рисков, чтобы увидеть, насколько вероятно, что они повлияют на организацию, и каковы могут быть последствия.
- **Риск управления** - определите методы, процедуры, технологии или другие меры, которые могут помочь организации снизить риски.
- **Анализируйте средства контроля** - на постоянной основе оценивайте, насколько эффективны средства контроля для снижения рисков, и добавляйте или корректируйте средства контроля по мере необходимости.

Оценка рисков кибербезопасности - это процесс, который помогает организациям определить ключевые бизнес-цели, а затем определить соответствующие ИТ-активы, необходимые для их реализации.

Он включает в себя выявление кибератак, которые могут негативно повлиять на эти ИТ-активы. От организации требуется определить вероятность возникновения этих атак и определить влияние, которое может оказать каждая атака.

Оценка рисков кибербезопасности должна отображать всю среду угроз и то, как она может повлиять на бизнес-цели организации.

Результат оценки должен помочь группам безопасности и соответствующим заинтересованным сторонам в принятии обоснованных решений о применении мер безопасности, которые снижают эти риски.

Что такое киберугрозы?

Термин киберугроза обычно применяется к любому вектору, который может быть использован для нарушения безопасности, нанесения ущерба организации или кражи данных.

Общие категории угроз, с которыми сталкиваются современные организации, включают:

- **Состязательные угрозы,** включая сторонних поставщиков, инсайдерские угрозы, доверенных инсайдеров, авторитетные хакерские коллективы, привилегированных инсайдеров, специальные группы, поставщиков, корпоративный шпионаж и национальные государства. В эту категорию также входят вредоносные программы (вредоносные программы), созданные любым из этих объектов. Крупные организации смягчают эти угрозы, создавая операционный центр безопасности (SOC) с обученным персоналом по безопасности и специализированными инструментами.
- **Стихийные бедствия** - ураганы, наводнения, землетрясения, пожары и молнии могут причинить такой же ущерб, как и злонамеренный кибер-злоумышленник. Стихийное бедствие может привести к потере данных, нарушению работы служб и разрушению физических или цифровых ресурсов организации. Угрозу стихийного бедствия можно минимизировать, распределив операции организации по нескольким физическим площадкам или используя распределенные облачные ресурсы.
- **Сбой системы - отказ** системы может вызвать потерю данных, а также привести к нарушению непрерывности бизнеса. Убедитесь, что ваши наиболее важные системы работают на высококачественном оборудовании, имеют резервирование для обеспечения высокой доступности, резервные копии, а ваши поставщики услуг предлагают своевременную поддержку.

- **Человеческая ошибка** - любой пользователь может случайно загрузить вредоносное ПО или попасть в ловушку с помощью схем социальной инженерии , таких как фишинговые кампании. Неправильная конфигурация хранилища может привести к раскрытию конфиденциальных данных . Чтобы предотвратить и смягчить эти угрозы, вам следует разработать программу обучения сотрудников и обеспечить строгие меры безопасности. Например, используйте менеджеры паролей и отслеживайте критические системы на предмет неправильной конфигурации.

Вот основные векторы угроз, которым подвержено большинство организаций:

- **Несанкционированный доступ** - может быть результатом действий злоумышленников, вредоносных программ и ошибок сотрудников.
- **Неправомерное использование информации авторизованными пользователями** - инсайдерская угроза может неправомерно использовать информацию, изменяя, удаляя или используя данные без разрешения.
- **Утечка данных** - злоумышленники или неправильная конфигурация облака могут привести к утечке личной информации и других типов конфиденциальных данных.
- **Потеря данных** - плохо настроенные процессы репликации и резервного копирования могут привести к потере или случайному удалению данных.
- Сбои в **обслуживании** - простой может привести к ущербу репутации и потере доходов. Это может быть случайность или результат атаки типа «отказ в обслуживании» (DoS).

Основы управления киберрисками

Существует несколько структур управления киберрисками, каждая из которых обеспечивает стандарты, которые организации могут использовать для выявления и снижения рисков. Высшее руководство и руководители

службы безопасности используют эти структуры для оценки и улучшения состояния безопасности в организации.

Структура управления киберрисками может помочь организациям эффективно оценивать, снижать и контролировать риски; и определить процессы и процедуры безопасности для их решения. Вот несколько часто используемых структур управления киберрисками.

NIST CSF

Структура кибербезопасности Национального института стандартов и технологий (NIST CSF) является популярной структурой. Структура NIST CSF предоставляет исчерпывающий набор передовых практик, стандартизирующих управление рисками. Он определяет карту действий и результатов, связанных с основными функциями управления рисками кибербезопасности - защита, обнаружение, идентификация, реагирование и восстановление.

ISO 27001

Международная организация по стандартизации (ISO) создала ISO / IEC 270001 в партнерстве с Международной электротехнической комиссией (IEC). Структура кибербезопасности ISO / IEC 270001 предлагает сертифицированный набор стандартов, определенных для систематического управления рисками, создаваемыми информационными системами. Организации также могут использовать стандарт ISO 31000, который содержит рекомендации по управлению рисками предприятия.

DoD RMF

Структура управления рисками (RMF) Министерства обороны (DoD) определяет руководящие принципы, которые агентства DoD используют при оценке и управлении рисками кибербезопасности. RMF разделяет стратегию управления киберрисками на шесть ключевых шагов: категоризация, выбор, внедрение, оценка, авторизация и мониторинг.

Честная структура

Структура факторного анализа информационных рисков (FAIR) определена с целью помочь предприятиям измерять, анализировать и понимать информационные риски. Цель состоит в том, чтобы направлять предприятия через процесс принятия обоснованных решений при разработке передовых методов кибербезопасности.

Лучшие практики для оценки рисков кибербезопасности

Встраивайте кибербезопасность в структуру управления рисками предприятия

Полностью включите свою программу кибербезопасности на основе рисков в структуру управления рисками предприятия, которая функционирует как организационный принцип для анализа и классификации рисков предприятия. Рамки следует использовать не как общее руководство, а как организующий принцип. Представляя киберриск как бизнес-риск, этот подход делает управление киберрисками более понятным для бизнеса.

Определите рабочие процессы, создающие ценность

Определите рабочие процессы, которые создают наибольшую ценность для бизнеса, и определите связанные с ними риски. Важно учитывать потенциальное влияние важнейших рабочих процессов, поскольку они также могут представлять значительный риск. Например, платежные процессы создают ценность, но представляют собой бизнес-риск, поскольку они уязвимы для мошенничества и утечки данных .

Убедитесь, что группа по кибербезопасности знает, какие процессы считаются ценными для вашей организации, и определите компоненты (активы данных, инструменты, группы), участвующие в каждом процессе. Это позволяет применять рекомендуемые элементы управления. Коллективный подход, включающий как кибербезопасность, так и бизнес-персонал, более эффективен, чем односторонний подход, основанный на зрелости.

Расставьте приоритеты киберрискам

Определите уровень риска на основе стоимости предотвращения и ценности информации для информирования ваших процедур управления

рисками и смягчения последствий. Риски высокого уровня следует рассматривать как можно скорее, тогда как риски низкого уровня могут быть устранены в дальнейшем или приняты как допустимые риски. Если стоимость защиты актива превышает его стоимость, затраты не окупаются, если только риск не может повлиять на вашу репутацию.

Осуществлять текущую оценку рисков

Выполняйте непрерывную, адаптивную и действенную идентификацию и оценку рисков, чтобы не отставать от возникающих угроз и решений кибербезопасности. Регулярно пересматривайте процессы управления рисками для выявления и устранения пробелов. Команды кибербезопасности полагаются на практические идеи, полученные от оценки рисков до защиты цифровых сред и активов.

Список литературы

1. Война в киберпространстве: уроки и выводы для России [Электронный ресурс] // Круглый стол в редакции «Независимого военного обозревателя». - Режим доступа : http://nvo.ng.ru/concepts/2013-12-13/l_war.html.
2. Госучреждения Германии страдают от хакерских атак [Электронный ресурс]. - Режим доступа : http://www.dw.de/ госучреждения-германии-страдают-от-хакерских-атак/a-16691699.
3. Дубов Д. Підходи до формування тезаурусу у сфері кібербезпеки / Д. Дубов // Політичний менеджмент. - 2010. - № 5. - С. 19-37.
4. Кибервойна: вымысел или реальность [Электронный ресурс] // Журнал Безопасность. - Режим доступа : http://www. securityinfowatch. ru/view.php? section=news&item= 121.
5. Кибернетическая безопасность и свобода информации [Электронный ресурс]. - Режим доступа : http://mediakritika.by/ article/kiberneticheskaya-bezopasnost-i-svoboda-informacii.
6. Ковалёв Н. «Началась новая техногенная эпоха - с кибервойнами, кибертерроризмом, киберпреступностью» [Электронный ресурс] / Н. Ковалёв

// Интервью для интернет-газеты «Столетия». - Режим доступа : http://www. stoletie.ru/.

7. Матвиенко Ю. А. Предупредить - значит вооружить (кибертерроризм вчера, сегодня и завтра) / Ю. А. Матвиенко // Геополитика. - 2011. - Вып. VI. - С. 59-82.
8. Мережко А. А. Конвенция о запрещении использования кибевойны в глобальной информационной сети информа-ционных и вычислительных ресурсов (Интернете) [Электронный ресурс] / А. А. Мережеко // Політичний менеджмент. - Режим доступа : http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57.
9. Министерство обороны США разрабатывает новые оперативные концепции защиты киберпространства [Электронный ресурс]. - Режим доступа : http://itstrateg.net/news/ministerstvo-oborony-ssha-razrabatyvaet-novye-operativnye-kontseptsii- zashchity-kiberprostranst.

Bibliography

1. War in cyberspace: lessons and conclusions for Russia [Electronic resource] // Round table edited by the Independent Military Observer. - Access mode: http://nvo.ng.ru/concepts/2013-12-13/l_war.html.
2. State institutions in Germany suffer from hacker attacks [Electronic resource]. - Mode of access : http://www.dw.de/ governmental-institutions-of-germany-suffer-from-hacker-attacks/a-16691699.
3. Dubov D. Approach to molding the thesaurus in the field of cybersecurity / D. Dubov // Political management. - 2010. - No. 5. - S. 19-37.
4. Cyberwar: fiction or reality [Electronic resource] // Journal of Security. - Access mode : http://www. security info watch. en/view.php? section=news&item=121.
5. Cybernetic security and freedom of information [Electronic resource]. - Access mode: http://mediakritika.by/article/kiberneticheskaya-bezopasnost-i-svoboda-informacii.

6. Kovalev N. “A new technogenic era has begun - with cyberwars, cyberterrorism, cybercrime” [Electronic resource] / N. Kovalev // Interview for the Internet newspaper “Centuries”. - Access mode : http://www. stoletie.ru/.
7. Matvienko Yu. A. To warn is to arm (cyberterrorism yesterday, today and tomorrow) / Yu. A. Matvienko // Geopolitika. - 2011. - Issue. VI. - S. 59-82.
8. Merezhko A. A. Convention on the prohibition of the use of cyber warfare in the global information network of information and computing resources (Internet) [Electronic resource] / A. A. Merezhko // Political management. - Access mode: http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57.
9. The US Department of Defense is developing new operational concepts for the protection of cyberspace [Electronic resource]. - Mode of access: http://itstrateg.net/news/ministerstvo-oborony-ssha-razrabatyvaet-novye-operativnye-kontseptsii-zashchity-kiberprostranst.

© Казарян К.К., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.

Для цитирования: Казарян К.К. УПРАВЛЕНИЕ РИСКАМИ КИБЕРБЕЗОПАСНОСТИ // Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.