ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Плюсы и минусы существующих подходов в оценке уровня защищённости организации

Александр Пушкин,
Заместитель генерального директора,
«Перспективный мониторинг»

Киберустойчивость – это способность ИС организации штатно функционировать в условиях воздействия компьютерных атак

Различные методики

CYBER RESILIENCE REVIEW (CRR)

NIST Cybersecurity Framework Crosswalks

The Cyber Resilience Blueprint: A New Perspective on Security

Еще один перечень критериев

Критерий	Пояснение
Инвентаризация ИТ	Знание и периодическая актуализация сведений по сетевым сегментам, ИС, СЗИ, хостам пользователей, внешнему периметру и их уровню значимости для реализации бизнес-процессов
Мониторинг ИТ/ИБ	Комплексное отслеживание, корреляция и анализ событий ИТ/ИБ для выявления индикаторов инцидентов на наиболее ранних этапах
Реагирование на инциденты	Созданы группы реагирования, подготовлены руководства по реагированию на актуальные для организации угрозы, проведение периодических учений
Оценка уровня защищенности	Знание и периодическая актуализация сведений по имеющимся недостаткам и уязвимостям ИТ. Налажен процесс устранения уязвимостей
Обеспечение непрерывности деятельности	Выработаны механизмы обеспечения непрерывности как для оборудования (резервирование, кластеризация), так и для информации (резервное копирование). Разработаны сценарии восстановления, проводятся периодические тренировки групп восстановления
Стратегия улучшения киберустойчивости	Подготовлена и реализуется Дорожная карта по улучшению основных и второстепенных критериев киберустойчивости

Подходы для оценки уровня защищённости

- Анализ защищённости
- Пентест
- Аудит

Цель

Анализ защищённости	Пентест	Аудит
Найти все известные и неизвестные уязвимости и недостатки, способные привести к нарушению конфиденциальности, целостности и доступности информации. Сформировать рекомендации по повышению уровня защищённости.	Достижение поставленной задачи. При этом вопрос полноты обнаруженных уязвимостей не стоит. Определить, может ли текущий уровень защищённости выдержать попытку вторжения потенциального злоумышленника с определённой целью.	Проверить, насколько информационная система (или её компоненты) и процессы соответствуют требованиям, лучшим практикам или рекомендациям нормативных актов, стандартов и документации производителей оборудования и ПО.

Фокус и уровень зрелости

Анализ защищённости	Пентест	Аудит
Важнее ширина исследования, чем глубина	Важнее глубина исследования, чем ширина	Важен объём выполнения требований и рекомендаций
От низкого до среднего	Высокий	От низкого до высокого

Критерии завершения

Анализ защищённости	Пентест	Аудит
Проект заканчивается по факту завершения проверок на наличие уязвимостей всех типов во всех подсистемах.	Проект заканчивается, как только поставленная цель будет достигнута или не достигнута из-за тех или иных причин (например, закончилось время, выделенное на проект).	Проект заканчивается по факту завершения всех проверок, предусмотренных методикой.

Методы достижения цели

Анализ защищённости	Пентест	Аудит
Исследования методом «чёрного / белого / серого ящика», анализ исходного кода, анализ структуры, функций, используемых технологий, подтверждение обнаруженных уязвимостей.	Все доступные методы и средства, удовлетворяющие ограничениям, поставленным заказчиком (в т. ч. социальная инженерия, атаки перебором и др.). Исследователи ищут кратчайший и самый дешёвый путь достижения целей.	Ручное или автоматизированное проведение проверок в соответствии с выбранной методикой.

Результат

Анализ защищённости	Пентест	Аудит
Максимально полный перечень обнаруженных уязвимостей.	Факт и/или вероятность взлома (проникновения) и получения информации злоумышленником.	Заключение о соответствии требованиям / рекомендациям.

От чего зависит стоимость

Анализ защищённости	Пентест	Аудит
От количества исследуемых сервисов, служб, приложений и протоколов, а также от модели угроз и нарушителя, методики проверки.	От комплексной сложности архитектуры, поставленных задач, сроков и ограничений на работу (например, работа только в выходные или ночное время).	От архитектуры и масштаба информационной системы, методики аудита и набора критериев.

Выводы

1. Тему киберустойчивости надо развивать и стандартизировать набор критериев оценки
2. Порог вхождения не должен быть высоким
3. Понимание особенностей подходов для оценки уровня защищенности позволяет сохранить время и деньги

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Александр Пушкин
Несергеевич

Заместитель генерального директора,

«Перспективный мониторинг»

t.me/pm_public amonitoring.ru ampire.team