УДК 004.056.55

ПЯТЬ УРОВНЕЙ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

Р.Ю. КАРАБАНОВ
(Представлено: канд. физ.-мат. наук, доц. Ю.Ф. ПАСТУХОВ)

Чтобы корректно защитить информацию в организации, необходимо иметь граммотную программу управления уязвимостями. Без такого пункта не обходятся ни одни рекомендации по обеспечению кибербезопасности на предприятии.

При рассмотрении этих пяти этапов будем основываться на модели зрелости возможностей (CMM, Capability Maturity Model), что в итоге должно дать вам представление о том, как вывести вашу организацию на новый уровень обеспечения информационной безопасности.

CMM переводится как "модель зрелости возможностей". Подразумевает модель зрелости процессов в компании. Изначально CMM была разработана для измерения эффективности работы подрядчиков, выполняющих заказы правительства США на разработку и поставку ПО. Позже модель была обобщена для любых компаний-разработчиков программного обеспечения.

Структура CMM. За основу при оценке способности организации качественно выполнять работу, которая (способность) была названа зрелостью, создатели модели взяли процессы организации. Дальше они сделали несколько нетривиальных предположений, которые впоследствии были приняты и признаны справедливыми многими ИТ-специалистами (а может быть, и большинством из них).

Предположение 1. Существуют качественно отличающиеся уровни зрелости проектной организации, разрабатывающей информационные системы (в модели CMM таких уровней пять).

Предположение 2. Всякая организация-разработчик заинтересована в переходе на более высокий уровень зрелости (не только для того, чтобы повысить свои шансы в борьбе за контракты Министерства обороны, но и в целях собственного совершенствования).

Предположение 3. Переход возможен только на следующий по порядку уровень. "Перескочить" через уровень нельзя (точнее, риски для организации при этом резко возрастают).

Таким образом, уровни образуют "лесенку", по которой подымается организация по мере собственного развития. Каждый уровень характеризуется определенными составом и свойствами процессов организации. "Лесенка уровней" CMM получила широкое признание и распространение. Вот как она выглядит (рис.).

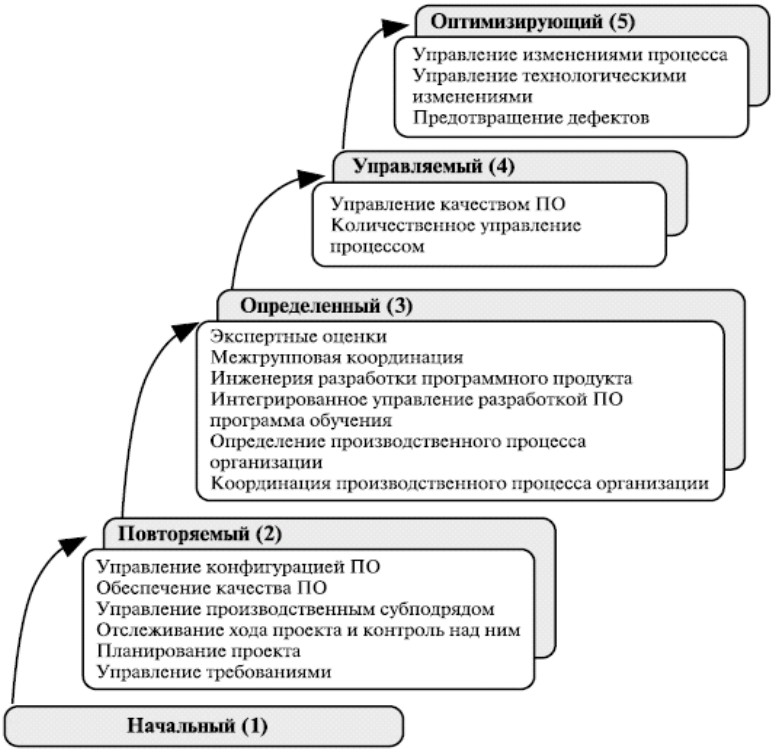

Рисунок. – Распределение групп ключевых процессов по уровням зрелости

Уровень 1: Начальный.

На начальном этапе программы управления уязвимостями процессы и процедуры либо отсутствуют полностью, либо присутствуют в минимальном наличии. Сканирование на уязвимости выполняется сторонним вендором как часть пентеста или внешнего сканирования. Такие тестирования обычно выполняются от одного до четырех раз в год по требованию аудитора, либо согласно нормативным требованиям.

Уровень 2: Повторяемый.

На этом этапе программы управления уязвимостями сканирование дыр в безопасности осуществляется внутри компании. Организация определяет набор процедур для сканирования брешей – обычно приобретается решение для управления уязвимостями, после чего сканирование проводится раз в неделю или в месяц, но на регулярной основе.

Большинство организаций, находящихся на этом этапе, не располагают поддержкой своего руководства, что приводит к тому, что бюджет на сканирование уязвимостей бывает крайне ограничен. Соответственно, приобретается относительно дешевое решение, либо используется бесплатный сканер уязвимостей с открытым исходным кодом.

Уровень 3: Установленный.

Этот уровень подразумевает, что программа управления уязвимостями качественно продумана и вся организация понимает ее. Команда компьютерной безопасности имеет поддержку со стороны руководства, а также располагает доверием системных администраторов. На этом этапе команда компьютерной безопасности уже выбрала надежное и безопасное решение для сканирования сети организации.

Согласно рекомендациям Center for Internet Security (CIS), на этом этапе сканирования проводятся минимум раз в неделю, а отчеты составляются индивидуально и доставляются на разные уровни организации. Таким образом, системные администраторы получают конкретные отчеты об уязвимостях, а менеджмент о тенденциях в этой области.

Данные о дырах в безопасности затем расшариваются с остальными отделами, завязанными на информационной безопасности, что позволяет обеспечить наличие оперативной информации. Например, если на внешнем брандмауэре обнаружен эксплойт, SIEM позволит быстро определить, какие системы уязвимы для этого эксплойта.

Уровень 4: Управляемый.

Здесь оцениваются конкретные атрибуты программы, а показатели предоставляются команде менеджмента. Можно выделить следующие показатели уязвимости, которые должна оценивать каждая организация:

Какой процент систем организации еще не подвергался сканированию системой управления уязвимостями?

Каков средний показатель уязвимости каждой из систем организации?

Каков общий показатель уязвимости каждой из систем организации?

Сколько времени в среднем занимает полное обновление прикладных программ для системы?

Эти показатели можно применять как к организации в целом, так и к отдельным подразделениям, что поможет понять, какие подразделения снижают риски, а какие отстают в этом вопросе.

Уровень 5: Оптимизированный.

На оптимизированном уровне метрики, определенные на предыдущем этапе, модернизируются. Оптимизация каждого из показателей способна обеспечить уменьшение поверхности для атаки. Команда безопасников должна работать совместно с менеджментом, чтобы установить определенные цели для программы управления уязвимостями.

Таким образом, обеспечение постоянного совершенствования вашей программы управления уязвимостями является ключом к уменьшению поверхности для атаки вашей организации. Если вам удастся уменьшить поверхность, вы поставите киберпреступников в затруднительное положение, им придется искать новые подходы и лазейки.

ЛИТЕРАТУРА

1. Пять этапов управления уязвимостями в организации [Электронный источник]. – 2018. – Режим доступа: https://www.anti-malware.ru/practice/methods/five-stages-of-vulnerability-management. – Дата доступа: 23.09.2018.
2. НОУ ИНТУИТ | Лекция | Зрелость проектных организаций. Методология CMM [Электронный источник]. – 2018. – Режим доступа: https://www.intuit.ru/studies/courses/2298/598/lecture/12857. – Дата доступа: 23.09.2018.
3. Криптографические основы безопасности [Электронный источник]. – 2017. – Режим доступа: http://www.intuit.ru/studies/courses/28/28/lecture/20412?page=4#sect17. – Дата доступа: 23.09.2018.
4. Что такое CMM? [Электронный источник]. – 2018. – Режим доступа: http://www.quizful.net/interview/qa/cmm. – Дата доступа: 23.09.2018.
5. Capability Maturity Model [Электронный источник] // Википедия. – 2018. – Режим доступа: https://ru.wikipedia.org/wiki/Capability_Maturity_Model. – Дата доступа: 23.09.2018.