УДК 004.627

МЕТРИКИ ПРОЦЕССА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Григорьева Виктория Андреевна, Тимофеев Дмитрий Сергеевич
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, vikylya_1992@mail.ru

В статье рассматриваются метрики информационной безопасности, особенности их применения и использования.

Ключевые слова – метрики, информационная безопасность, управление инцидентами.

ВСТУПЛЕНИЕ

Метрика – это количественное измерение, которое может быть интерпретировано в контексте ряда предыдущих измерений или эквивалентных измерений [1]. Метрики необходимы для того, чтобы

- показать, каким образом деятельность по безопасности вносит непосредственный вклад в достижение целей;
- измерить, как изменения в процессе отражаются на достижении основных целей;
- выявить существенные аномалии в процессах и принять обоснованные решения по исправлению или улучшению процессов.

Один из наиболее значимых процессов в системе управления информационной безопасностью - управление инцидентами, под которым понимается восстановление нормальной работоспособности системы в максимально короткие сроки и минимизация отрицательного влияния на бизнес, пользующийся сервисами, работоспособность которых оказалась нарушенной.

ОСНОВНАЯ ЧАСТЬ

Рассматривая метрики безопасности можно утверждать, что они должны быть воспроизводимыми. Это означает, что, применив при оценке один и тот же метод и одинаковый набор исходных данных, разные специалисты должны получить эквивалентные результаты, т.е. они не должны зависеть от субъективных суждений экспертов. Помимо этого, не стоит забывать, что метрики все-таки надо высчитывать. Важно, чтобы периодичность их оценки и усилия, прикладываемые к их вычислению, были сопоставимы. Не нужно усложнять формулы метрик, которые оцениваются достаточно часто. Также следует избегать качественных значений для метрик, необходимо стремиться к их количественному выражению. Качественные значения, такие как "низкий", "средний", "высокий", могут использоваться для наглядности, например, в презентациях для руководства. Но они всегда должны быть только лишь дополнением к количественным оценкам и ни в коем случае не заменять их. Необходимо также отметить, что правильно сформулированные метрики должны иметь выражение в неких единицах измерения, связанных с оцениваемой величиной.

Выполняя все эти рекомендации при формулировании метрик, важно не забыть самое главное – они должны быть конкретными, ясными, иметь непосредственное отношение к измеряемому процессу. А также быть направленными на то, чтобы результаты их оценки давали как можно больше информации: что не так в проблемной зоне и как изменить ситуацию к лучшему.

Существует пять этапов использования метрик: измерение, представление, интерпретация, исследование и диагностирование. Каждый из этих этапов рассмотрим на примере процесса управления инцидентами.

1. Измерение: измерение текущего значения метрики выполняется на периодической основе и обычно выполняется в определенный промежуток времени. Например: посмотреть какие произошли инциденты в процессе управления за отчетный период на предприятии и насколько быстро была восстановлена информация.

2. Интерпретация: измеренное значение оценивается в сравнении с пороговым или целевым, либо иным сопоставимым. Обычно на предприятии ставятся пороговые значения и ведется наблюдение за отклонениями. Нормальные значения, расположенные между пороговыми, оцениваются на основании статистических или сопоставимых данных. В результате интерпретации можно выделить следующие факторы:

- **Аномалии**: когда измеренная величина выходит за пределы допустимых пороговых значений. Указывается пороговое значение, например 2, если это значение превышено, то это и будет аномалия.
- **Успех**: когда измеренная величина оказывается ниже целевой. Если после диагностики не выявлено отклонений или они лучше предполагаемого значения, можно сказать что это успех.
- **Тенденция**: основное направление изменения значений произведенных измерений по отношению к цели. Главной целью предприятия является беспрерывная работа, если в случае диагностики количество инцидентов уменьшается, то эффективность работы возрастает.
- **Ориентир для сравнения**: относительная позиция измерения или тенденция среди равнозначных измерений. В случае сравнения произведенных диагностик, смотрим насколько улучшилась или ухудшилась работоспособность предприятия.

3. Расследование: расследование аномальных результатов измерений в идеале заканчивается

выявлением основных причин такого значения метрики, например, после диагностики проводится анализ имеющихся отклонений, нарушений с определением первопричины их возникновения. Такими могут быть результаты принятых управленческих решений, или особые причины (ошибки, атаки, аварии).

4. Представление: надлежащая визуализация метрики имеет ключевое значение для ее правильной интерпретации. Представление метрик изменяется в зависимости от типа сравнения и распределения ресурсов. Чаще всего итоговые результаты представляются в виде столбчатых диаграмм, круговых диаграмм и графики. С помощью них становится лучше видно какие проблемы существуют на данном предприятии.

5. Диагностирование: руководителям следует использовать результаты предыдущих этапов для диагностирования ситуации, анализа альтернатив и их последствий, а также для принятия бизнес-решений. После проведения исследований результаты передаются руководителю, а он сравнивает результаты с предыдущими диагностиками и предпринимает решения по улучшению работы предприятия.

ВЫВОДЫ

Разрабатывая процесс оценки эффективности ИБ, организация должна быть готова к необходимости принятия управленческих решений и их выполнения. Возможно, даже не только в части ИБ. Только в этом случае оценка эффективности с использованием метрик становится гибким и удобным инструментом для оценки процессов и мер обеспечения ИБ. Причем здесь можно говорить как о мелких корректировках отклонений в эффективности конкретных мер по ИБ, так и о необходимости существенных изменений. Их внедрение позволяет обеспечить работу процессов информационной безопасности в соответствии с ожиданиями и целями бизнеса, рационально расходуя ресурсы. При этом всегда есть возможность отслеживать, приносят ли прилагаемые усилия необходимый результат.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Метрики безопасности / Способ доступа: URL: http://pathfinder1.livejournal.com/105989.html. – Загол. з екрана.

2. Оценка эффективности и метрики ИБ / Способ доступа: URL: http://www.itsec.ru/articles2/control/ocenka-effektivnosti-i-metriki-ib/ – Загол. з екрана.