Аналитическое чтение тезисов с лекции 2 (от 16 фев 2015)

Мартынов Семён

10 марта 2015 г.

Селеста Лин Пол, известный эксперт в области дизайна и юзабилити, а также член совета KDE e.V. в своём отчёте по человекоориентированному изучению Сетевых Операционных центров (СОЦ) публикует те методики и приёмы, которые, по её мнению, могут помочь будущим исследователям этой области.

Она начинает с того, что перечисляет те сложности, с которыми сталкивается человек, исследующий сетевую безопасность с точки зрения работы людей, и главным из них является сложность сбора информации, т.к. специалисты, занимающиеся сетевой аналитикой, постоянно перегружены задачами и у них нет времени отвлекаться от своей работы. Тем не менее, растет общее понимание, что в компьютерной безопасности человеческий фактор превалирует над технологией, так что подобные исследования необходимы.

Своё исследование она проводила в крупном правительственном Сетевом Центре, занимавшемся обеспечением защиты крупной правительственной сети. Работа в центре строилось по принципу 24/7 и делилась на две смены (дневную и ночную). Доступ в подобные организации строго ограничен, и для проведения исследования требовалось приглашение кого-либо из Центра или партнерской организации.

В виду особенностей изучаемой среды, автору требовались гибкие методы работы с минимальным влиянием на саму среду. Интервью, полевые исследования и распределение карточек длилось более 12 месяцев.

Первые **интервью** были проведены с целью понимания работы Сетевого Операционного центра ещё до визита на объект. Базовую информацию (границы ответственности, используемые средства, общая организация) могла быть получена от человека, имевшего достаточный опыт работы в центре. Эти темы хорошо подходят для первой встречи с новым человеком, хотя и не являются самым эффективным способом потратить время интервьюируемого специалиста.

Семь интервью были проведены в людьми, имевшими опыт работы в СОЦ. Интервью содержали открытые вопросы чтобы не ограничивать экспертов. Продолжительность каждого интервью была от 45 минут до полутора часов. Последние три интервью были с людьми, которые на тот момент работали в центре в должности начальника смены. Это те люди, кто выполнял операционные задачи и принимал решения в течение смены. Среди трёх интервьюируемых нашёлся человек заинтересовавшийся исследованием, и

обеспечивший автору доступ на объект. Проведённые интервью позволили составить понимание целей и методов работы операционных центров а так же получить базовые знания до погружения в эту среду.

Примерно 30 часов были посвящены **наблюдению**. Оно проводилось один раз в месяц по 2 – 4 часа. Как правило, наблюдение проводилось в ночное время, т.к. дневные смены очень заняты другими посетителями и встречами. Ночные смены тише, и иногда предоставляют возможность общения с аналитиком при минимальном влиянии на работу.

Наблюдение включало следующие активности:

- Ежедневные операции, включая совместную работу и коммуникации между аналитиками и менеджерами
- Плановые встреча, летучки и технические демонстрации
- Тренировочные упражнения, изображающие различные события

Распределение карточек является методом, позволяющим человеку выстроить связи между объектами, и построить ментальную модель обсуждаемой области. Автор задавала вопрос и просила аналитиков и менеджеров разбить карточки на группы по применяемым для решения этого вопроса методам. Когда участник заканчивал, он описывал каждую группу и объяснял свой выбор.

Аналитики и менеджеры получали удовольствие от участия в этом эксперименте. После недели работы, они ощутили себя частью исследования. Некоторые участники отметили, что задача с карточками подтолкнула их к общим размышлениям о той области, к которой они были хорошо знакомы.

Результаты работы с карточками легли в основу другого исследования по анализу работы процессов и позволили выявить, что аналитики и менеджеры считают наиболее важным в своей работе.

В итоге, автор заключает, что Сетевые Операционные центры являются средой с высокой степенью взаимодействия сотрудников. Хотя каждый аналитик имеет свою зону ответственности, общая работа строится на командном принципе. Наиболее применяемым методом распространения информации является вербальное общение. Обычной ситуацией является когда аналитик подходит к столу другого аналитика, или несколько человек собираются вместе для обсуждения какого-либо вопроса, даже если каждый из них видит на своём мониторе одну и туже картинку. Наиболее важная информация может распространяться по внутренней телефонной связи. Менее приоритетная информация фиксировалась в виде каких либо артефактов, которые можно было передать следующей смене.

Подобная система создаёт трудности для обмена данными между сменами. Использование тикетов и отчётов о событиях не позволяет передать контекст ситуации. Наиболее эффективно подобные данные хранятся в "капитанском журнале который ведёт начальник смены. Но реальная возможность ведения таких записей сильно связана с тем, на сколько напряженная выдалась смена.

Наиболее сложным аспектом работы начальника смены является поддержание необходимого уровня осведомлённости о состоянии сети. Он должен собрать воедино все единичные инциденты, и на основании этой работы предоставить отчёт сво-

ему руководству. И это именно то место, где использование новых инструментов и артефактов способно улучшить результаты.

В конце, Селеста перечисляет три основных урока, которые она извлекла.

- Продолжительные исследования. Необходимо разработать долгосрочный план и следовать ему длительный период времени. Частые посещения центра более эффективны чем полноценное внедрение в его работу, т.к. минимизирует влияние на исследуемую среду. Частота посещений должна быть достаточной для поддержания отношений с сотрудниками и быть в курсе последних событий, но не так часто, чтоб отвлекать внимание служащих.

- Смешение методов. Один активный метод может дать быстрый результат, но окажет негативный эффект на исследуемую среду. Несколько не больших исследований можно раскидать на разные периоды и скорректировать по мере проведения научно-исследовательского проекта. Разнообразие техник является хорошей практикой.

- Заводите друзей. Развивайте и поддерживайте профессиональные дружеские отношения с людьми, которых вы изучаете. Слишком близкие отношения может привести к конфликту интересов, но и отсутствие дружеских отношений может иметь критические результаты - здесь автор говорит о начальнике смены, который обеспечил ей доступ в СОЦ.

Рассказ о трёх Центах управления инцидентами Информационной Безопасности (ЦИБ) публикует группа из пяти авторов. Как и автор первого материала, они говорят о важности человеческого фактора в вопросах безопасности и жалуются на высокую загруженность специалистов. В то же время, они критикуют интервью как не достаточно полный и объективный механизм исследования, и идут по пути внедрения своих специально подготовленные студентов на реальные объекты.

Первый студент на два месяца отправился работать аналитиком первого уровня в ЦИБ некой корпорации, имеющую интересы по всему миру. В зоне ответственности этого ЦИБа находилось порядка 350'000 сетевых устройств на территории США. Задача центра была определена как наблюдение, анализ и устранение последствий значительных событий информационной безопасности. Оперативная группа состоит из 20 аналитиков и 2 аналитиков второго уровня, во главе группы находится менеджер. Каждый аналитик работает 4 дня в неделю и 10 часов в день. Каждый сутки разделена на три смены, а расписание планируется так, чтобы в каждой смене участвовало минимум 2 аналитика первого уровня. В своей работе они используют wiki и систему тикетов. За эти два месяца студенту довелось столкнуться с настоящими инцидентами информационной безопасности - в одном случае речь шла об обнаружении SQL-инъекции на одном веб-сервере, в другом автоматическая система безопасности обнаружила распространение вируса, под видом терминального клиента.

Второй студент стажировался в ЦИБ другой корпорации в должности аналитика безопасности. Корпоративный ЦИБ использует внутренние и сторонние средства для обес-

печения реакции первого уровня и подтверждения угрозы информационной безопасности с минимальным воздействием на бизнес. В данном случае ЦИБ распределён по всему миру для обеспечения режима работы 24x7x365 и быстрой реакции на инциденты. Миссией ЦИБ является восстановление и поддержание нормальной работы и безостановочного производства, повышение уровня безопасности и надёжности, сдерживание и предотвращение инцидентов в будущем (вплоть до судебного преследования).

Третьему студенту повезло меньше всех и он проходил стажировку в своём ВУЗе. Под управлением ВУЗовского ЦИБа было 50'000 устройств по всему студенческому городку. Большинство аналитиков в этом ЦИБе специализировались на каких-то конкретных задачах, но были и общие задачи, такие как фиксация инцидентов и выполнение задач от других аналитиков. По своим задачам, аналитики делились на 4 группы:

- A1 – проведение экспертиз
- A2 – управление брандмауэром, VPN, и архитектура сетевой безопасности
- A3 – управление брандмауэром и управление индустрией платёжных систем
- A4 – задачи платёжных систем и общее руководство

В итоге выявляется стандартный набор проблем, таких как поддержка связи между аналитиками ночной смены и остальной частью команды. Работа по сбору информации в ЦИБах продолжается, и, возможно, в будущем будут более интересные результаты.

Исследованием результатов работы этичных хакеров по программе раскрытия уязвимостей в интернете занялась группа из трёх исследователей.

Этичные хакеры вносят значительный вклад в область кибербезопасности, представляя публичные отчёты по уязвимости по программ вознаграждения. Авторы материала провели анализ данных за последние три с половиной года работы Китайской фирмы: 3'254 этичных хакера предоставили отчёты о 16'446 уязвимостях в интернете.

Авторами были выявлены следующие тренды:

- Активность этичных хакеров опережает их общий рост
- Большинство уязвимостей кроется на мелких сайтах

Авторы предлагают не ограничиваться на изучении технических деталей уязвимостей и разработке новых инструментов анализа, но и понять как охотники за уязвимостями совершают свои открытия.