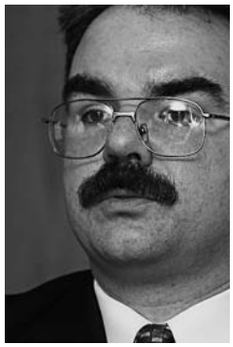
SPECIAL ОПРОС



АЛЕКСЕЙ ЛУКАЦКИЙ
Бизнес-консультант по безопасности «Cisco Systems». В «Cisco» отвечает за развитие направления безопасности в России и странах СНГ.

АЛЕКСАНДР АНТИПОВ
Руководитель проекта, автор/соавтор/корректор многочисленных статей ведущего отечественного портала по информационной безопасности *SecurityLab.ru*.

АНТОН ПАЛАГИН
Директор по развитию компании «Eykon». Его первая должность — как раз администратор.

ЗАРАЗА
Руководитель службы поддержки пользователей довольно крупного ISP. Хобби — разработка программного обеспечения, в частности проект «3proxy» (*www.security.nnov.ru/soft/3proxy/*).

КОНСТАНТИН ГАВРИЛЕНКО
Консультант по безопасности и по совместительству директор компании «Архонт». Специализируется на безопасности сетевой инфраструктуры и безопасности беспроводной связи.

У АДМИНИСТРАТОРА СЛОЖНЫЙ ГРАФИК РАБОТЫ. СБОИ И АТАКИ МОГУТ БЫТЬ КАК ДНЕМ, ТАК И НОЧЬЮ. КАК БЫТЬ?

ЗАРАЗА: Это все определяется масштабами фирмы. Крупная компания может себе позволить дежурного администратора, который будет на рабочем месте и ночью. Помельче — администратора, который будет дежурить дома с трубкой в пределах досягаемости... Ну а если это компания, которой не выгодно иметь более одного администратора, то можно и одного администратора не брать. А заказать услуги администрирования организации, которая этим занимается профессионально, и в штате которой — несколько администраторов. То есть отдать администрирование на аутсорсинг. Тогда можно и отпусков не бояться...

ЧТО САМОЕ ГЛАВНОЕ В АДМИНИСТРИРОВАНИИ?

ЗАРАЗА: В администрировании все главное. Любая ошибка, сделанная администратором, не важно на каком этапе — планирования или реализации — может обернуться большими, очень часто невосполнимыми, потерями. Поэтому очень важно, чтобы задачи, которые решает системный администратор, были четко сформулированы и находились в пределах его компетенции. Ошибки в системном администрировании чаще всего делаются руководителями. Они рассуждают так: «я ничего в этом не понимаю, поэтому я найму технического человека, пусть он решает все технические вопросы». В резуль-

тате получается, что технический специалист начинает заниматься решением задач постановки технологического процесса, то есть совсем не технических. Кроме того, его действия никому не подконтрольны. Никто не может оценить качество работы.

При правильной организации системного администрирования все действия администратора четко регламентированы и подотчетны. Любое действие в системе происходит не само по себе, а по какому-то документу. Это снимает большую часть ответственности с администратора и перекладывает ее на того, кто подписал документ. Такая «бюрократизация» процедуры системного администрирования устраняет необдуманные действия со стороны администратора, значительно снижая вероятность ошибки. Постановка системного администрирования — это как раз и есть весьма трудоемкая задача по превращению набора неких хаотических и плохо понятных действий в хорошо отлаженный процесс.

АЛЕКСАНДР АНТИПОВ: Самое главное — выполнять все распоряжения начальства! Кто такой системный администратор? Человек подневольный, которого не замечают, когда все нормально работает, и на которого сыпятся все шишки, если что-то сломалось. Хорошо, если только сломалось, и он смог быстро решить возникшую проблему. Например, часто оказывается, что после того, как в течение месяца вдруг резко уменьшается поток писем от возможных клиентов компании, начальство узнает об установленном спам-фильтре. И тут бесполезно рассказывать про заботу о пользователях, постоянно жалующихся на увеличенное количество спама, — все равно окажешься виноватым, так как твоя инициатива нанесла прямой ущерб бизнесу.

Бывает плохой админ, хороший админ, а бывает правильный админ. Плохой — это тот, у которого ничего и никогда нормально не работает, а виноват в этом всегда Билл Гейтс и его глючные Винды. Хороший админ тихо делает всю свою работу, получает шишки от начальства и никогда не добьется повышения зарплаты или более высокой должности. Правильный же админ всегда перед тем, как нажать на кнопку, напишет внутреннюю инструкцию по тому, как нужно нажимать на эту кнопку, напишет докладную записку начальнику с аргументами о необходимости нажатия этой кнопки (пусть начальник представляет отделу продаж твои аргументы), а только потом нажмет на нее. Правильный админ всегда будет на хорошем счету у начальства, никогда не будет виноват и, вполне вероятно, быстро дослужится до более высокой должности с более высокой зарплатой.

АНТОН ПАЛАГИН: Главное для администратора — не становиться священной коровой, к которой несут дароносицу. К несчастью, это случается слишком часто, и зарвавшегося администратора приходится менять, со всеми вытекающими отсюда последствиями. Так что получается, что самое главное умение администратора — это умение взаимодействовать с людьми. Недаром на должность, так сказать, «штатского» администратора всегда назначают приятных и умеющих общаться девушек. На приличном ресепшене сидит человек, который тебе всегда поможет и подскажет, а не обложит матом и не попросит литр пива и рыбки к нему за ерундовую услугу.

Соответственно, для объекта администрирования важно, чтобы людям было удобно работать. Девушку Таню ведь не волнуют проблемы безопасности, связанные с дырками в IIS 6.0, ей интересно послушать музыку и посплетничать с соседкой Ксюшей о новом галстуке начальника. Но она не может сделать этого, потому что администратор Эммануил считает, что аська несет потенциальную угрозу безопасности. Бред? Конечно. А если начальник Зиновий Галактионович считает, что использование аськи пагубно сказывается на удоях... тьфу, то есть на работоспособности, то хороший администратор должен убедить его в обратном. Потому что девушки все равно будут сплетничать (с помощью гугл-тока или просто в туалете), и на работоспособность это никак не повлияет.

И, конечно, безопасность, — от нее никуда не денешься. Скажи мне, пожалуйста, о какой безопасности можно говорить, если сложный пароль секретарша записывает на бумажку и кладет ее под клавиатуру или наклеивает на монитор. А если ее за это отругать, то она сменит пароль на «123», чтобы было проще запомнить. И здесь администратор должен проявить умение общаться и убеждать (учить) секретаршу пользоваться специальными программами для записи конфиденциальной информации. Так что хороший администратор, в моем понимании, это тот, кто умеет решать проблемы пользователей, а не создавать им проблемы. Тогда глядишь, коллеги не будут зло смеяться над его внешностью, грязными ногтями и желтыми от кофе и курева зубами. Этих атрибутов просто не будет. А еще я за то, чтобы администратора, как и футбольного арбитра, не было заметно.

КОНСТАНТИН ГАВРИЛЕНКО: На этот вопрос невозможно дать однозначный ответ, и выделить единственный архиважный компонент. Принцип администрирования определяется ИТ-политикой компании, и в зависимости от этого можно определить некоторые направления, которые и будут являться доминирующими в работе администратора.

В первую очередь, любой человек, занимающийся администрированием, должен руководствоваться двумя основными принципами: стабильность и безопасность. Следом за ними идут функциональность и автоматизация. На самом деле, все четыре составляющие достаточно тесно переплетены между собой. Квалифицированный администратор должен уметь просчитать последствия во взаимодействии перечисленных составных частей от изменений, вносимых в структуру администрируемого объекта.

Но вне зависимости от типа администрируемой сети и потенциального материального ущерба от ее взлома, безопасность является одним из наиболее важных компонентов. Степень безопасности напрямую воздействует, по крайней мере, на стабильность и функциональность. Для каждой из других частей, при условии самого неприятного исхода, существует возможность исправить и вернуть все на свои места. В случае с безопасностью такая возможность отсутствует.

Останавливаясь на качествах администратора, особо стоит отметить отсутствие туннельного мышления и нестандартного подхода к решению проблем. А также любви к пицце, кофе и хорошему пиву.

АЛЕКСЕЙ ЛУКАЦКИЙ: В администрировании главное — планирование, как бы непривычно это не звучало. Причем планирование не в его советском понимании, а классический план, включающий в себя ответы на вопросы:

— ЧТО И ЗАЧЕМ НАДО СДЕЛАТЬ (ПО-КРУПНОМУ)?
ОТВЕТ НА ЭТОТ ВОПРОС ДОЛЖЕН БЫТЬ ТЕСНО СВЯЗАН С ЦЕЛЯМИ ОРГАНИЗАЦИИ. НАПРИМЕР, ВНЕДРЕНИЕ IP-ТЕЛЕФОНИИ ПОЗВОЛИТ СЭКОНОМИТЬ НА МЕЖДУГОРОДНИХ ПЕРЕГОВОРАХ И ПОЛУЧИТЬ НОВЫЕ ПРЕИМУЩЕСТВА ОТ ИСПОЛЬЗОВАНИЯ ТЕЛЕФОНИИ (НАПРИМЕР, ИНТЕГРАЦИЯ С CRM-СИСТЕМОЙ И ПОЛУЧЕНИЕ ВСЕЙ ИСТОРИИ ЗАКАЗОВ ИЛИ TROUBLESHOTING CASE'ОВ ЗВОНИВШЕГО).

— ЧТО НАДО СДЕЛАТЬ КОНКРЕТНО?
ДАЛЬШЕ МЫ ОПРЕДЕЛЯЕМ КОНКРЕТНЫЕ ДЕЙСТВИЯ, ПОЗВОЛЯЮЩИЕ ДОСТИЧЬ ПОСТАВЛЕННОЙ ЗАДАЧИ.

— КОГДА ЭТО НАДО СДЕЛАТЬ, И КТО ЭТИМ ЗАЙМЕТСЯ?
УСТАНАВЛИВАЕМ СРОКИ И ОТВЕТСТВЕННЫХ. ЕСЛИ ОРГАНИЗАЦИЯ НЕБОЛЬШАЯ, ТО ОТВЕТСТВЕННЫЙ ВСЕГДА БУДЕТ ТОЛЬКО ОДИН.

— КАК ИЗМЕРИТЬ ЭФФЕКТИВНОСТЬ?
ЭТО ОЧЕНЬ ВАЖНЫЙ МОМЕНТ, КОТОРЫЙ ОБЫЧНО ИЗ ВИДУ УПУСКАЕТСЯ. СДЕЛАТЬ ЧТО-ТО — СДЕЛАЛИ, А ВОТ ПРОВЕРИТЬ, НАСКОЛЬКО СДЕЛАННЫЕ ИЗМЕНЕНИЯ КОРРЕКТНЫ И ПРИВОДЯТ К НУЖНОМУ РЕЗУЛЬТАТУ, ЗАБЫВАЮТ. ИНОГДА РЕЗУЛЬТАТ, ТАК СКАЗАТЬ, НАЛИЦО. НО ЗАЧАСТУЮ ПРИХОДИТСЯ ПРОВОДИТЬ ДОСТАТОЧНО СЛОЖНЫЕ ИССЛЕДОВАНИЯ И ИСПЫТАНИЯ, ЧТОБЫ ПОНЯТЬ, ЧТО ВСЕ РАБОТАЕТ «КАК ЗАДУМАНО».

И только после ответа на все эти вопросы надо переходить непосредственно к конкретным действиям, которые многие и понимают как истинное администрирование **C**