Визитка

АЛЕКСЕЙ ДРОЗД,
руководитель отдела информационной безопасности «СёрчИнформ»

Раз-два-три-четыре-пять, сисадмин ушел гулять

Как не развалить офис, когда сисадмин вне зоны доступа

Сисадмины, как и другие сотрудники, в любой момент могут, запланировано или нет, выбыть из рабочего процесса. Как не остаться «как без рук», когда сисадмин в отпуске или на больничном?

Даже на ключевых позициях сотрудники не должны быть незаменимы. Хорошо, если ИТ-отдел большой, – один выбыл, другие подхватили, никаких простоев. Если вы давно сотрудничаете с крупным аутсорсером, там хватает сотрудников на замену, если ответственный за вашу компанию будет отсутствовать. Но если в штате только один специалист или компания работает с одним фрилансером, а он по какой-то причине окажется вне доступа, возникнут проблемы.

Мы знаем, насколько проще и дешевле восстановить данные из RAID 1, чем из единственного, посыпавшегося HDD. Настолько же надежней иметь бэкап-план на случай отсутствия сисадмина, чем срочно искать и приглашать «гуру», когда все пойдет наперекосяк. Поэтому заранее проведите тотальный аудит и подготовьте шпаргалки как обеспечить устойчивость инфраструктуры.

Вот, что придется сделать.

Об авторе

Алексей Дрозд – Начальник отдела информационной безопасности «СёрчИнформ».

Опыт работы в ИТ и ИБ – 9 лет. Прошел путь от системного администратора до руководителя проектов.

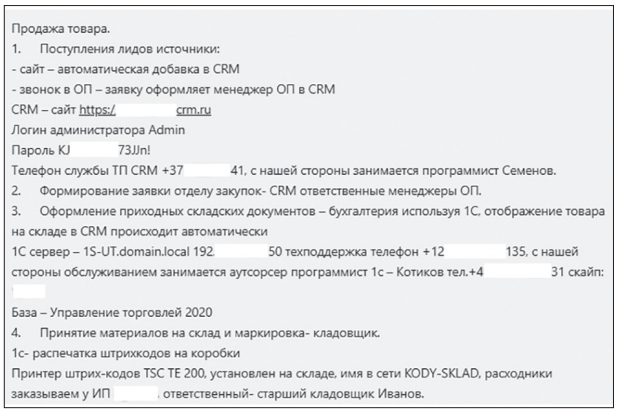
Автор учебных программ по администрированию и практике применения DLP-систем для специалистов по информационной безопасности. Составитель учебно-методического комплекса, который применяется в 65 вузах СНГ для обучения по специальностям «Информационная безопасность», «Компьютерная безопасность», «Информационная безопасность телекоммуникационных систем», «Информационная безопасность автоматизированных систем», «Информационно-аналитические системы безопасности», «Экономическая безопасность». В 2014 году принимал участие в создании учебно-методических материалов для программы подготовки магистров в рамках международного проекта Tempus, Educating the next generation experts in Cyber Security.

Специализируется на темах, находящихся на стыке психологии и информационной безопасности (корпоративное мошенничество, социальная инженерия и т. п.). Автор публикаций для российских научных журналов.

Модератор, спикер и участник профильных форумов «Код ИБ», Tadviser, Road Show SearchInform, международных научных конференций по информационной безопасности.

Шаг 1. Устраиваем «перепись всего»:

- **Проводим инвентаризацию** всего компьютерного оборудования.
- **Документируем топологию сетей:** общую, локальные подсети отделов, рабочий и «гостевой» Wi-Fi.
- **Бэкапируем конфигурацию сетевых устройств:** логины, пароли, настройки от всех свитчей, маршрутизаторов, роутеров и точек Wi-Fi.
- **Описываем бизнес-процессы** и задействованные в них элементы ИТ-инфраструктуры. Должна получиться памятка примерно такого вида:



Продажа товара.
1. Поступления лидов источники:
- сайт – автоматическая добавка в CRM
- звонок в ОП – заявку оформляет менеджер ОП в CRM
CRM – сайт https:/ crm.ru
Логин администратора Admin
Пароль KJ 73JJn!
Телефон службы ТП CRM +37 41, с нашей стороны занимается программист Семенов.
2. Формирование заявки отделу закупок- CRM ответственные менеджеры ОП.
3. Оформление приходных складских документов – бухгалтерия используя 1С, отображение товара на складе в CRM происходит автоматически
1С сервер – 1S-UT.domain.local 192. 50 техподдержка телефон +12 135, с нашей стороны обслуживанием занимается аутсорсер программист 1с – Котиков тел.+4 31 скайп:
База – Управление торговлей 2020
4. Принятие материалов на склад и маркировка- кладовщик.
1с- распечатка штрихкодов на коробки
Принтер штрих-кодов TSC TE 200, установлен на складе, имя в сети KODY-SKLAD, расходники заказываем у ИП , ответственный- старший кладовщик Иванов.

Иными словами, описываем сам процесс, сервисы и оборудование, которые в нем задействованы, пишем имена ответственных в отделе (об этом ниже) и со стороны айтишников – со всеми контактами.

- **Ведем учет** активным и «спящим» учетным записям в AD и корпоративных сервисах, в том числе указываем права доступа к критическим ресурсам и их настройкам. Лучше перестраховаться и бэкапить эти данные вручную – прямо по старинке, в табличку или на листок бумаги.

Шаг 2. Автоматизируем рутину

- **Настраиваем бэкапирование** корпоративных сервисов в сетевые хранилища с помощью специального софта

или хотя бы встроенными средствами ОС. Задаем расписание для создания резервных копий – как правило, оптимально делать это раз в сутки.

- **Настраиваем автоматическое обновление** всех критически важных сервисов, ОС, средств защиты (антивирусов, файрволов, антиспамов и пр.). Если ПО платное, лучше удостовериться, что у него продлена и работает техподдержка.
- **Настраиваем систему бесперебойного питания,** подключаем к ней ключевые устройства и прописываем настройки на случай внезапного отключения. На многих серверах это можно сделать перед первым запуском: заранее предусмотрите, как будет происходить перезапуск и восстановление сеансов в критических ситуациях.
- **Прописываем скрипты для сложных операций,** которые непрофильные сотрудники не смогут выполнить самостоятельно. Например, программу, которая автоматически отправит модем на перезагрузку при неполадках сети. Или развернет бэкап сервера в случае потери данных. Технически написать такую программу несложно, но важно составить к ней инструкцию, как к «большой красной кнопке»: в каких случаях запускать скрипт, что делать дальше. И заранее выдать права на запуск скриптов доверенным пользователям. Например, завести вторую учетку для директора, где на рабочем столе будет единственный ярлык «Перезапустить почтовый сервер».

Шаг 3. Налаживаем коммуникацию

- **Заранее обучаем сотрудников** работе с ПО. Тогда бухгалтеры не запаникуют, когда 1С выдает предупреждение о смене учетной даты, и смогут без помощи сисадминов нажать «ОК». И с оборудованием – тогда на складе не растеряются и перезагрузят зависший сканер.
- **Назначаем ответственных «администраторов»** в каждом отделе, наиболее опытных в работе с нужным ПО. Именно им придется в экстренной ситуации запускать «антикризисные» скрипты от сисадминов. Проверяем, чтобы они знали, как это сделать и где взять доступы к учеткам с правами запуска этих программ.
- **Проводим общий ликбез** о том, когда действительно нужно обращаться в техподдержку или срочно доставать сисадмина из инфекционного карантина, а с какими проблемами можно справиться самостоятельно. Обновляем контакты с вендорами и передаем их ответственным сотрудникам.

Наконец, главное

Шаг 4. Создаем папку «Судного дня»

По моему опыту, ни один сисадмин не уйдет в отпуск, не проложив себе «коридор» для удаленного доступа к рабочим сетям. И даже на больничную койку ложится, готовый выйти на связь. Поэтому довольно сложно представить ситуацию, когда компания окажется совсем обездоленной. И все же лучше перестраховаться. Поэтому –

- **Пакуем в архив все до мелочей:** пути к сетевым ресурсам и хранилищу бэкапов, перечень оборудования с указанием моделей устройств, указания, какие порты на свитчах задействованы во VLAN. Туда же – логины и пароли от корпоративных сервисов, перечень учеток, а еще контакты всех ответственных сотрудников, аутсорсеров и инженеров техподдержки со стороны вендоров. Словом, всю информацию, которую собрали на предыдущих этапах.

Лучше подготовить такую «папку» одновременно на флешке/внешнем диске и в бумажном виде. И оперативно вносить туда все происходящие изменения. Храниться папка и флешки должны буквально за семью печатями – например, в сейфе директора.

Такая информация пригодится и в рядовой ситуации, например, когда в ИТ-отдел приходит новичок или меняется подрядчик аутсорсинга. С помощью этих бумаг им будет легче разобраться в происходящем и сразу приступить к задачам.

Если же ситуация действительно экстренная, а сисадмин вне доступа, привлекайте помощь со стороны. Обратитесь к аутсорсерам в любом формате – хоть одолжите знакомого спеца из «соседнего офиса» и передайте им все шпаргалки. Главное, чтобы все действия «варягов» в вашей корпоративной сети логировались, еще лучше – просматривались «вживую».

> Технически написать такую программу несложно, но важно составить к ней инструкцию, как к «большой красной кнопке»: в каких случаях запускать скрипт, что делать дальше

Для этого можно использовать DLP и SIEM-системы, системы аудита для файловых хранилищ и БД. Они позволяют защититься от недобросовестных действий даже привилегированных пользователей, держать в сохранности данные, в ряде случаев – конфигурацию оборудования. При этом системы контроля необязательно закупать дополнительно.

Если у компании нет свободных ресурсов, можно привлечь ИБ-аналитиков в формате аутсорсинга, а системы арендовать (сейчас, в условиях кризиса, вендоры предлагают услугу бесплатно). Так и коллектив, и все временные «сменщики» окажутся под присмотром – ниже риск, что смогут случайно или намеренно навредить компании. А когда штатный сисадмин вернется в строй, по отчетам без труда разберется, что делали помощники в его отсутствие. EOF

[1] Чек-лист по организации безопасного удаленного доступа: https://searchinform.ru/uploads/sites/1/2020/03/chek-list-po-perehodu-na-udalenku.pdf
[2] 10 правил хорошего тона в организации IT-инфраструктуры: https://searchinform.ru/blog/2019/11/05/10-pravil-horoshego-tona-v-organizaciiit-infrastruktury/
[3] Руководство по созданию системы резервного копирования: https://habr.com/ru/post/421251/

Ключевые слова: бэкап, аудит, удаленный доступ, системы контроля, СёрчИнформ