ISSN 1560-5191 01
9 771560 519127

Коммуникации для бизнеса

сети network world

ТЕМА НОМЕРА: средства коллективной работы

www.osp.ru/nets №1 (268) март 2012

Иллюстрация: МегаФон

Быстро и повсеместно

Параметры сети 3G позволяют работать в мобильном режиме практически с любым контентом из электронной почты и бизнес-приложений, утверждает Константин Солодухин, заместитель генерального директора по развитию федеральных корпоративных продаж и операторского бизнеса ОАО «МегаФон», генеральный директор компании «Синтерра». Стр. 7

АЛЕКСЕЙ ЕСАУЛЕНКО

Полезная «матрица»

Одно из самых необычных помещений в калифорнийском исследовательском центре компании Cisco ее сотрудники в шутку прозвали матрицей. Речь идет о тестовой лаборатории, стены которой имеют весьма своеобразную «отделку».

Вместо окрашенного гипсокартона или пластиковых панелей здесь использована сплошная комбинация из нескольких сотен жидкокристаллических и плазменных мониторов и такого же количества видеокамер с микрофонами.

Все это оборудование представляет собой серийные образцы продуктов Cisco для видеоконференций и телеприсутствия.

В соседнем зале находится сердце этого испытательного стенда — несколько стоек с вычислительными и коммуникационными серверами, ответственными за агрегацию сигналов от видеокамер и последующее распределение мультимедийных потоков на мониторы.

Система функционирует таким образом, что на каждом экране «матрицы» может отображаться видео с любой из сопряженных с ней камер, и внешне это поразительно напоминает эффектные кадры из культовой ленты о компьютерной симуляции реальности.

Управляя трафиком опытной системы, инженеры могут имитировать сотни вариантов проведения видеоконференций с участием десятков тысяч терминалов. В этом и заключается ее основное предназначение — отработка сложных нестандартных сценариев применения видеосистем для совместной работы больших пользовательских групп.

Первый вопрос, который приходит в голову после ознакомления с экспериментами Cisco в Кремниевой долине: найдутся ли заказчики для испытываемых здесь гиперсложных систем видеосвязи и существуют ли в природе приложения, в которых требуется подключение такого огромного количества экранов и камер?

Представители компании поясняют: возможно, столь масштабные системы и не будут востребованы на практике, но нужна уверенность, что в случае возникновения необходимости все тестируемые в лаборатории продукты Cisco окажутся на высоте.

Любопытно, что именно Россия оказалась первой в мире страной, где была реализована во многом похожая на «матрицу» Cisco гигантская сетевая инфраструктура. В ее состав включены десятки тысяч видеокамер и миллионы пользовательских мониторов, соединенных с общими центрами обработки данных.

Мы говорим о нашумевшем проекте оснащения избирательных участков камерами видеонаблюдения. Специалисты признают, что по уровню сложности и масштабам применения видеосистем он не имеет себе равных в мире.

Задачи этого проекта в определенном смысле идентичны тем, что ставили перед собой испытатели из Cisco, — обеспечить совместную работу множества пользователей. Ведь выборный процесс — это большая коллективная работа по формированию государственной власти в стране.

И пусть политики спорят о том, в какой мере выборный процесс в России превратился в симуляцию реальности.

Мы же отметим, что беспрецедентный опыт построения инфокоммуникационной системы такого масштаба действительно может принести большую пользу стране, поскольку созданная для выборов ИТ-инфраструктура впоследствии может быть использована, например, для организации облачных сервисов в сферах образования и здравоохранения или для других крупных инициатив, где группы людей действуют сообща. Первый в этом году выпуск *«Сетей»* посвящен средствам коллективной работы (Collaboration).

СОДЕРЖАНИЕ

сети/network world

Главный редактор
Алексей Есауленко *esaul@osp.ru*

Над номером работали
Валерий Коржов, Владимир Болдырев, Леонид Черняк, Людмила Яремчук, Павел Иванов

Специальный корреспондент в С.-Петербурге
Дмитрий Желвицкий

Литературные редакторы
Нина Михеева, Софья Ямпольская

Корректор Людмила Теременко

Компьютерная верстка и графика
Алексей Быков

Отдел рекламы
Елена Лушникова *lushnik@osp.ru*

Служба распространения и подписки
xpress@osp.ru

Адрес редакции: 123056, Москва, Электрический пер., д. 8, стр. 3, «Сети»

Телефоны:
(499) 253-9229, 956-3306 — редакция;
(495) 725-4785 — подписка;
(495) 725-4785 — распространение;
(499) 253-9116/17, 956-3306 — отдел рекламы;
(495) 783-9366, (49651) 73179 — типография

Факс: (499) 253-9204/05

E-mail: *nets@networld.ru*

Учредитель
IDG, 1 Exeter Plaza, Massachusets 02116, USA

Издатель
ЗАО «Издательство «Открытые системы»
109072, Москва, ул. Серафимовича, д. 2, к. 3

Президент Михаил Борисов

Генеральный директор Галина Герасина

Коммерческий директор Татьяна Филина

Издание зарегистрировано в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций.
Рег. № 01053 от 18.12.1995

Подписной индекс
40991 (каталог «Пресса России»);
99492 (каталог «Почта России»).

Цена свободная

Отпечатано в ООО «Богородский полиграфический комбинат», 142400, Московская область, г. Ногинск, ул. Индустриальная, д. 40б

Системы видеоконференций требуют внимательной настройки

Директор компании Rapid7 по вопросам безопасности обнаружил тысячи уязвимых систем видеоконференций

ГРЕГ КЕЙЗЕР
Computerworld, США

Десятки тысяч систем видеоконференций, включая те, которые организуются из переговорных комнат в офисах компаний, где обсуждается в том числе и закрытая информация, уязвимы для шпионских атак.

Об этом предупреждает директор компании Rapid7 по вопросам безопасности HD Мур. По его выражению, многие системы видеоконференций фактически выставляют своих участников напоказ в Интернете.

Мур не один месяц пытался «запустить щупальца» в самые дорогие программные и аппаратные системы видеоконференций и посетил не одну переговорную. Опасность, по его мнению, исключительно велика, а ее причина — безответственный подход к настройке инструментов защиты.

С помощью инструментов сканирования Мур обследовал небольшой сектор Интернета с целью обнаружить аппаратное обеспечение, использующее протокол H.323, наиболее широко распространенный при организации видеоконференций. Он выяснил, что 2% этих устройств подвергались серьезному риску со стороны хакеров, поскольку были настроены давать автоматический ответ на любой входящий звонок и не были защищены сетевым экраном.

В Интернете в целом Мур насчитал свыше 150 тыс. систем видеоконференций, уязвимых для прослушивания с помощью аппаратных микрофонов и камер с удаленным управлением.

Наиболее частая ошибка при настройке систем видеоконференций состоит в том, что не отключается функция автоматического ответа, и аппаратное обеспечение устанавливается либо без сетевого экрана, либо вне обычного периметра защиты предприятия. Впрочем, даже если системы защиты формально используются, сетевые экраны недостаточно хорошо работают с протоколом H.323, и система остается уязвимой для проникновения.

Уязвимости системам видеоконференций добавляет еще и то, что некоторые программные средства поддержки видеоконференций для имеющегося оборудования, приобретенные через такие магазины, как eBay, не очищаются от предустановленных соединений с другими точками проведения конференций.

Муру удавалось получить доступ к видеоконференциям, проводящимся в залах заседаний советов директоров компаний, к совещаниям в исследовательских лабораториях, юридических фирмах и венчурных фондах.

В одном случае Муру удалось дозвониться до идущей конференции и получить управление камерой. Манипулируя камерой, он настроился на портативный компьютер одного из участников, чтобы в подходящем увеличении увидеть, как тот набирает пароль. Все это происходило в течение 20 минут, и никто в комнате не заметил, что камера двигается как бы сама по себе.

Некоторые производители систем видеоконференций не согласны с доводами Мура о простоте шпионажа.

Дэвид Малдоу, аналитик компании Telepresence Options, специалист консультационной фирмы Human Productivity, специализирующейся на развертывании систем видеоконференций, усомнился в том, что Мур просто «набирал случайные номера и ходил по каким-то пустым комнатам». Мур опроверг это утверждение.

«Я был поражен, насколько плачевна ситуация с видеоконференциями, — заявил Мур. — Популярность видеоконференций превратила целый ряд компаний в мишени для промышленного шпионажа или получения сведений, обеспечивающих конкурентные преимущества».

Иллюстрация: Cisco

ЗЛОУМЫШЛЕННИКИ МОГУТ получить доступ к видеоконференциям, проводящимся в залах заседаний советов директоров компаний. Поэтому даже самая совершенная система видеоконференц-связи требует тщательной настройки