PCWEEK UKRAINIAN EDITION
Pelican Publishing
ГАЗЕТА ДЛЯ КОРПОРАТИВНЫХ ПОЛЬЗОВАТЕЛЕЙ ИТ
• 6 сентября — 20 сентября 2012 №14 (36) • КИЕВ

КОНФЕРЕНЦИЯ PCWEEK/UE
DATACENTRE EVOLUTION
Проектирование. Оптимизация. Аутсорсинг
КИЕВ, 18 октября
Регистрация на сайте pcweek.ua

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ОБЪЁМНЫЙ ВЗГЛЯД

ВИРТУАЛЬНАЯ ПЛАТФОРМА БИЗНЕС-КЛАССА

ВИРТУАЛЬНЫЙ СЕРВЕР В ЕВРОПЕ

Защита бизнеса от технических и административных рисков
Значительное повышение конкурентоспособности
Катастрофоустойчивая ИТ-инфраструктура
Масштабируемая ИТ-инфраструктура

- **Виртуальный сервер**
- ОЗУ 4 ГБ
- HDD 80 ГБ (дублированный)
- 100 Мбит/с канал
- Мониторинг сети
- 24x7 русскоязычная поддержка

215 EUR в месяц

+ Установка **БЕСПЛАТНО**
+ **РЕПЛИКАЦИЯ** данных
+ **GOLD SLA** Время реакции - 2 часа

Доступны также другие конфигурации.

Виртуальная платформа DEAC основана на новейших решениях

EMC² vmware hp DELL

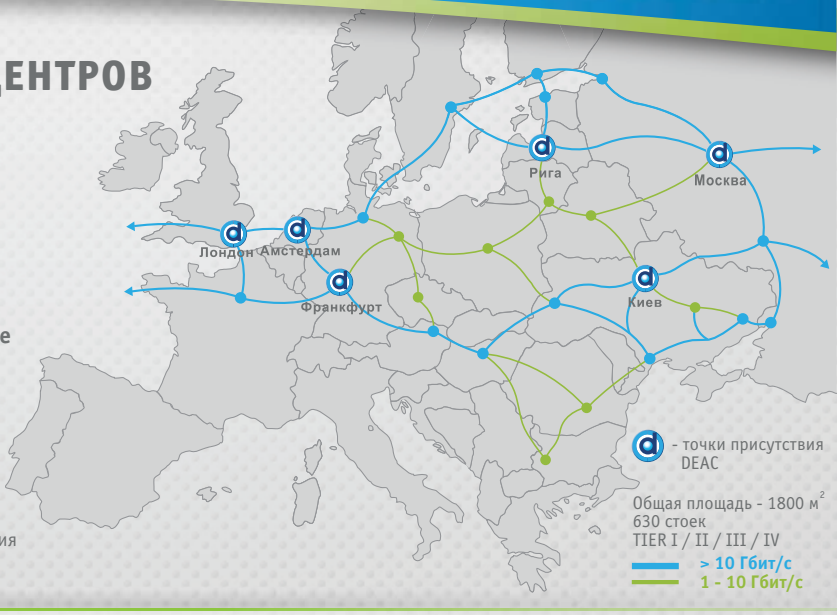
ЕВРОПЕЙСКИЙ ОПЕРАТОР ДАТА-ЦЕНТРОВ

deac ИТ аутсорсинг

office@deac.eu
WWW.DEAC.EU
WWW.DEACDC.RU

Виртуальный тур по дата-центрам DEAC

Корпоративное видео DEAC



Центральный офис: ул. Маскавас 459, Рига, Латвия
Тел.: +371 6707 2100 Моб.: +371 2946 6055

Представительство в РФ: ул. Садовническая 82, п-д 6, офис 2058, Москва, Россия
Моб.: +7 926 448 2657

Предлагаем Вам встретиться с DEAC на мероприятиях:

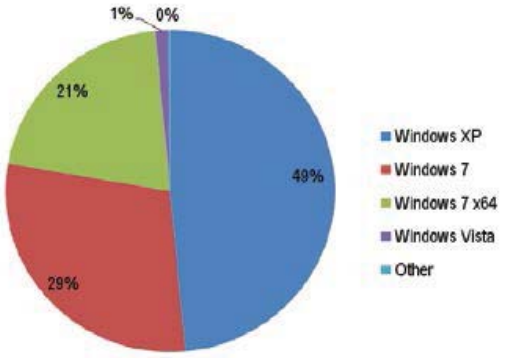
Форум "Вокруг ЦОД, вокруг IP"	Киев	27.09.2012	„PCWEEK ЦОД 2012“	Киев	18.10.2012
Ялтинское заседание ИТ-директоров	Ялта	7-10.10.2012	„Круглый стол финансовых директоров“	Мальта	1-4.11.2012

ЗАЩИТА ДЛЯ ОНЛАЙН-ШОПИНГА

ОЛЕГ ПИЛИПЕНКО

По прогнозам IDC, в текущем году будет совершено около одного миллиарда онлайн-покупок на общую сумму более 1,2 трлн долл. Почти 80% пользователей в мире приобретают товары через Интернет, 69% регулярно работают с системами онлайн-банкинга. В нашей стране ситуация несколько иная. Исследование, проведенное «Лабораторией Касперского» в Украине, свидетельствует, что покупки через Интернет с помощью ПК совершают 55% пользователей, а онлайн-банкинг применяют 39%.

По словам Виталия Камлюка, ведущего антивирусного эксперта «Лаборатории Касперского», при онлайн-платежах пользователи сталкиваются с такими рисками, как ввод личных данных на фишинговых сайтах и несанкционированная установка троянцев, похищающих конфиденциальную информацию. Возможен также перехват секретных сведений кейлоггерами при вводе данных на клавиатуре.

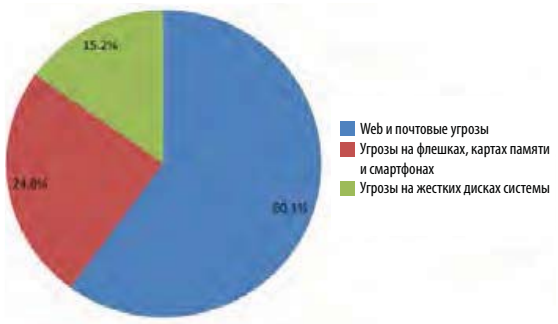


Распределение уязвимостей по платформам

Отвечая на усиливающийся натиск онлайн-угроз, компания «Лаборатория Касперского» в новой линейке продуктов для домашних пользователей основной акцент сделала на защите личных данных пользователя при совершении покупок в Интернете, а также любых банковских онлайн-операций. Традиционно перед началом бизнес-сезона разработчик представил два продукта: решение для комплексной безопасности Kaspersky Internet Security 2013 и продукт для базовой защиты «Антивирус Касперского 2013».

В обновленном KIS 2013 применено несколько совершенно новых методик для борьбы с наиболее распространенными и сложными угрозами, нацеленными на личные данные и банковские счета пользователя. Важнейшие из них — технологии «Безопасные платежи» и «Автоматическая защита от эксплойтов».

Технология «Безопасные платежи» предусматривает широкий набор методов защиты при проведении финансовых операций через Интернет. В их число входят онлайн-покупки, работа с электронными системами платежей, например, «Яндекс.Деньги», а также доступ к банковскому счету с компьютера. Функция автоматически включается при посещении наиболее популярных платежных и банковских сайтов, проверяет подлинность сайта самой платежной системы и состояние безопасности компьютера пользователя. Также новый инструмент защиты предлагает открыть сайт в специальном защищенном режиме, в котором контролируется доступ других программ и процессов к передаваемым данным для их защиты от кражи. Стоит отметить и новую технологию защиты ввода данных с аппаратной клавиатуры: в ней используется специальный драйвер для предотвращения регистрации нажатий клавиш вредоносными программами при вводе информации с обычной, а не виртуальной клавиатуры.



Ситуация в Украине — распределение угроз

Для защиты пользователей от фишинга в состав обоих продуктов входит модуль «Анти-фишинг». Среди его функций — автоматическое обновление и улучшенное эвристическое детектирование сайтов, на которых злоумышленники пытаются украсть пароли и другие ценные данные пользователя. В состав Kaspersky Internet Security 2013 также входит новое ядро анти-спама для обнаружения нежелательных писем в электронной почте.

Технология «Автоматическая защита от эксплойтов» разработана для противодействия наиболее сложным и опасным угрозам — тем, что используют неизвестные или незакрытые уязвимости в популярных программах. Новая разработка позволяет защитить пользователей продуктов «Лаборатории Касперского» от подобных эксплойтов, в том числе использующих так называемые уязвимости нулевого дня.

В основе KIS 2013 и «Антивируса Касперского 2013» лежит новое антивирусное ядро, обеспечивающее более высокое качество обнаружения всех видов вредоносных программ, включая самые сложные образцы. В частности, в нем реализованы конкретные методы для эффективной борьбы с комплексными и целевыми угрозами путем нейтрализации попыток внедрить вредоносный код в ключевые системные процессы. В то же время в новых продуктах обновления баз стали быстрее и меньше по объему, поскольку определенные их части перенесены в облако.

Технология «Автоматическая защита от эксплойтов» разработана для противодействия наиболее сложным и опасным угрозам

Kaspersky Internet Security 2013 и «Антивирус Касперского 2013» уже доступны для приобретения. Стоимость продуктов составляет 486 и 340 грн на 2 ПК на 1 год соответственно.

HP ПРЕДЛАГАЕТ ПЕЧАТАТЬ БОЛЬШЕ

ОЛЕГ ПИЛИПЕНКО

ПЕРВЫЙ ВЗГЛЯД

До середины 90-х годов прошлого века технологии офисной печати развивались быстрыми темпами, однако далее прогресс в этой области несколько замедлился. За последнее десятилетие производители не смогли изобрести какую-либо принципиально новую технологию печати. Поэтому при разработке новых устройств основной упор вендоры сделали на снижение себестоимости печати, а также их оснащение беспроводной связью, возможностью печати через Интернет или напрямую с мобильных устройств.

Еще в минувшем году компания HP представила свою фирменную технологию ePrint. Суть её заключается в том, что каждому принтеру HP с доступом в Интернет присваивается свой уникальный адрес электронной почты типа ***@hpeprint.com.

Пользователи мобильных телефонов, смартфонов и планшетных компьютеров устанавливают на своем мобильном устройстве специальное приложение-клиент, которое прикрепляет файл к письму и отправляет на почтовый ящик печатающего устройства. Посредством беспроводной связи документ загружается на принтер и распечатывается. Таким образом, гаджеты, никогда не подключаемые к принтерам, при помощи ePrint получают возможность печати. Среди поддерживаемых вложений — документы Microsoft Word, Excel, PowerPoint, JPEG, Adobe PDF, а также файлы HTML.

МФУ HP Deskjet Ink Advantage 4625 e-All-in-One ориентировано на бизнес-пользователей, нуждающихся в универсальном устройстве для печати, сканирования, копирования документов, отправки факсов

В новой серии печатных устройств Deskjet Ink Advantage, недавно представленной в Украине, компания HP сделала основной упор на технологиях беспроводной печати и снижении себестоимости отпечатка при общем повышении производительности. Модельный ряд с пятью новинками нацелен на домашних пользователей и представителей микробизнеса.

Устройство начального уровня Deskjet Ink Advantage 2515 отличается компактными размерами и доступной ценой. Новинка класса «все-в-одном» ориентирована на домашних пользователей, позволяет легко печатать, сканировать и копировать документы и фотографии. Скорость печати составляет до 8 стр./мин. в черно-белом режиме и до 5 стр./мин. в цветном.

МФУ Deskjet Ink Advantage 3525 e-All-in-One и 5525 e-All-in-One оснащены Wi-Fi для печати с мобильных гаджетов. Кстати, благодаря технологии HP wireless direct printing пользователи могут печатать, даже не имея беспроводного маршрутизатора. Оба устройства соответствуют стандарту ENERGY STAR и могут снизить расход бумаги до 50% с помощью функции автоматической двусторонней печати и копирования. Кроме того, модель Deskjet Ink Advantage 5525 e-All-in-One также оснащена функцией сканирования и отправки файлов на электронный ящик без использования компьютера.

Модель HP Deskjet Ink Advantage 5525 e-All-in-One оснащена функцией сканирования и отправки файлов на электронный ящик без использования компьютера

Модели Deskjet Ink Advantage 4615 All-in-One и 4625 e-All-in-One ориентированы на бизнес-пользователей, нуждающихся в универсальном устройстве для печати, сканирования, копирования документов, отправки факсов высокого качества по низкой цене. Новинки оснащены механизмом автоматической подачи оригиналов для сканирования с лотком на 35 страниц. Благодаря функции Scheduled On/Off экономия потребляемой энергии составляет до 40%. Максимальная скорость монохромной печати — 8 стр./мин., цветной печати — 7,5 стр./мин.; разрешение при сканировании — 1200x1200 dpi.

Стоит отметить, что модели 3525 e-All-in-One, 5525 e-All-in-One и 4625 e-All-in-One позволяют дистанционно печатать документы с помощью технологии HP ePrint. Такая функция значительно расширяет возможности принтера.

Как заявили представители HP, себестоимость печати одной страницы в новой линейке Deskjet Ink Advantage снизилась в два раза. Это стало возможным благодаря использованию в новинках более емких картриджей HP 650 и HP 655. Оригинальные картриджи HP позволяют напечатать до 600 страниц, вместо 300 страниц в старых моделях.

Многофункциональное устройство Deskjet Ink Advantage 2515 доступно в продаже по рекомендованной цене 649 грн. Модели Deskjet Ink Advantage 3525 и 5525 e-All-in-One уже поступили на полки магазинов по рекомендованной цене 999 грн и 1299 грн соответственно.

МФУ Deskjet Ink Advantage 4625 e-All-in-One доступно для покупателей по рекомендованной цене 1499 грн, а Deskjet Ink Advantage 4615 All-in-One — за 1199 грн.

При использовании материалов ссылка на сайт pcweek.ua обязательна

PCWEEK UKRAINIAN EDITION

СОДЕРЖАНИЕ

НОВОСТИ

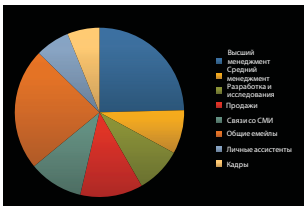
3 Защита для онлайн-шопинга

3 HP предлагает печатать больше

7 «Фабрика печати» на новый лад

ТЕМА НОМЕРА

8 Защита данных: объемный взгляд



10 Оградиться от инсайдеров

12 Средство контроля для высшей касты

13 Більшість людей думає лише про зручність, а не про безпеку

14 IPv6 и сетевая безопасность

14 Бизнес рискует, переводя конфиденциальные данные в облачные системы хранения

КОРПОРАТИВНЫЕ СИСТЕМЫ

16 Неудобная правда о резервном копировании

18 Прогнозируя будущее корпоративного ИТ-рынка

20 Облачные вычисления: 10 изменений к 2020 г.

21 Бизнес на аккумуляторах

22 Развертывание облачных систем с открытым исходным кодом

АНОНСЫ

- **Тема номера: новые имена на ИТ-рынке Украины**
- **Интервью с Пер-Гуннар Остби, региональным вице-президентом по развивающимся рынкам компании Quest Software**
- **Отчет о конференции «Information Security 2012: Миссия выполнима»**
- **Windows 8 Enterprise: превью RTM-версии**
- **Интервью с Михаилом Дробиком, UC&C продакт-менеджером компании Huawei**

Новости вашей компании, мнения о наших публикациях, приглашения на конференции и семинары, ваши пожелания высылайте по адресу: press@skukraine.com

НОВОСТИ

ИТ-СТРАТЕГИЯ

AMD о будущей эре вычислительного окружения

Технологический руководитель AMD Марк Пейпермастер обрисовал на конференции Hot Chips свое видение возрастающей интеллектуальности окружающих человека вещей.

Руководители Advanced Micro Devices начали говорить о предстоящем приходе, как они выражаются, Surround Computing Era (Эры вычислительного окружения) — картины будущего с мириадами вычислительных интерфейсов и насыщенных интеллектом устройств, присутствующих во всем, начиная с ПК и бытовых устройств до автомобилей и предметов одежды.

Это видение, изложенное на недавней конференции Hot Chips 2012 старшим вице-президентом и директором AMD по технологии Марком Пейпермастером, отражает тренд, который некоторые компании называют «Интернетом вещей», а Intel — «Вычислительным континуумом» (Compute Continuum). Однако AMD также говорит о том, что клавиатура и мышь уступят место интерфейсам с безупречным распознаванием голоса и черт лица, а компьютеры, облака и растущее число вездесущих сенсоров смогут обрабатывать в реальном времени гигантские объемы данных. Интеллектуальность новых вычислительных сред, считает Пейпермастер, непосредственно повлияет на жизнь людей.

В корпоративном блоге AMD Пейпермастер еще до презентации на Hot Chips опубликовал пост, в котором привел возможный пример функционирования Вычислительного окружения:

«Допустим, в полдень вы собирались выйти из офиса перекусить. При выходе на улицу ваше мобильное устройство интуитивно распознает, куда вы направляетесь, автоматически анализируя поток данных от встроенных GPS-навигатора, часов, карт и подключенной облачной базы данных. Поскольку ему также известны ваши предпочтения, оно соединится с сайтом вашего любимого ресторана и проверит наличие фирменных блюд. Из устройства прозвучит доброжелательный автоматический голос с предложением заказать обед. Вы назовете нужное блюдо, и устройство отправит за вас заказ. В момент, когда вы придете в ресторан, для вас уже все готово. Заказ был оплачен электронным образом, пока вы были в пути, и вам даже не надо доставать бумажник. И для всего этого не надо загружать специальные приложения или пользоваться клавиатурой телефона».

Это станет результатом дальнейших разработок во многих областях, включая облачные среды для хранения данных, мощные серверы для функционирования датацентров и разнообразные устройства для взаимодействия с конечным пользователем. Сюда также относятся ПО и сервисы, которые сделают Surround Computing реальностью.

Сама AMD уже вносит вклад в эти разработки, начиная с гибридных процессоров (APU), соединяющих на одном кристалле вычисления и графику, и заканчивая продолжающими совершенствоваться центральными и графическими процессорами. Это направление, написал Пейпермастер, также потребует создания мощных вычислительных сеток микросерверов, примером которых являются продукты SeaMicro, купленной в этом году AMD за 334 млн долл., и стандартного ПО, постоянно обновляемого тысячами разработчиков.

Дискуссия о Surround Computing была частью графика напряженной недели, которую руководство AMD использовало для обсуждения в ходе конференций Hot Chips и VMworld 2012 будущих планов и анонса новых предложений. В ходе Hot Chips Пейпермастер также рассказал о будущем процессорном ядре Steamroller, идущем на смену нынешнему ядру Piledriver. Steamroller, которое позволит выпускать более быстрые и эффективные процессоры, появится в будущем году в 28-нанометровых двух- и четырехъядерных APU для ПК с кодовым названием Kaveri.

БИЗНЕС

GROUP-IB и CS заключили соглашение о партнерстве

Компания CS, ведущий украинский разработчик систем автоматизации банковской деятельности, и Group-IB, российская компания, занимающаяся расследованием компьютерных преступлений, объявляют о заключении партнерского соглашения. Партнерство направлено на усиление противодействия хищениям в системах интернет-банкинга на территориях России и Украины.

В рамках подписанного соглашения компании договорились об участии в совместных проектах, направленных на снижение уровня компьютерных преступлений на финансовом рынке Украины. В первую очередь это касается объединения усилий в профилактике случаев хищений денежных средств с помощью систем дистанционного банковского противодействия атакам и проведения совместных мероприятий, нацеленых на снижение хакерской активности.

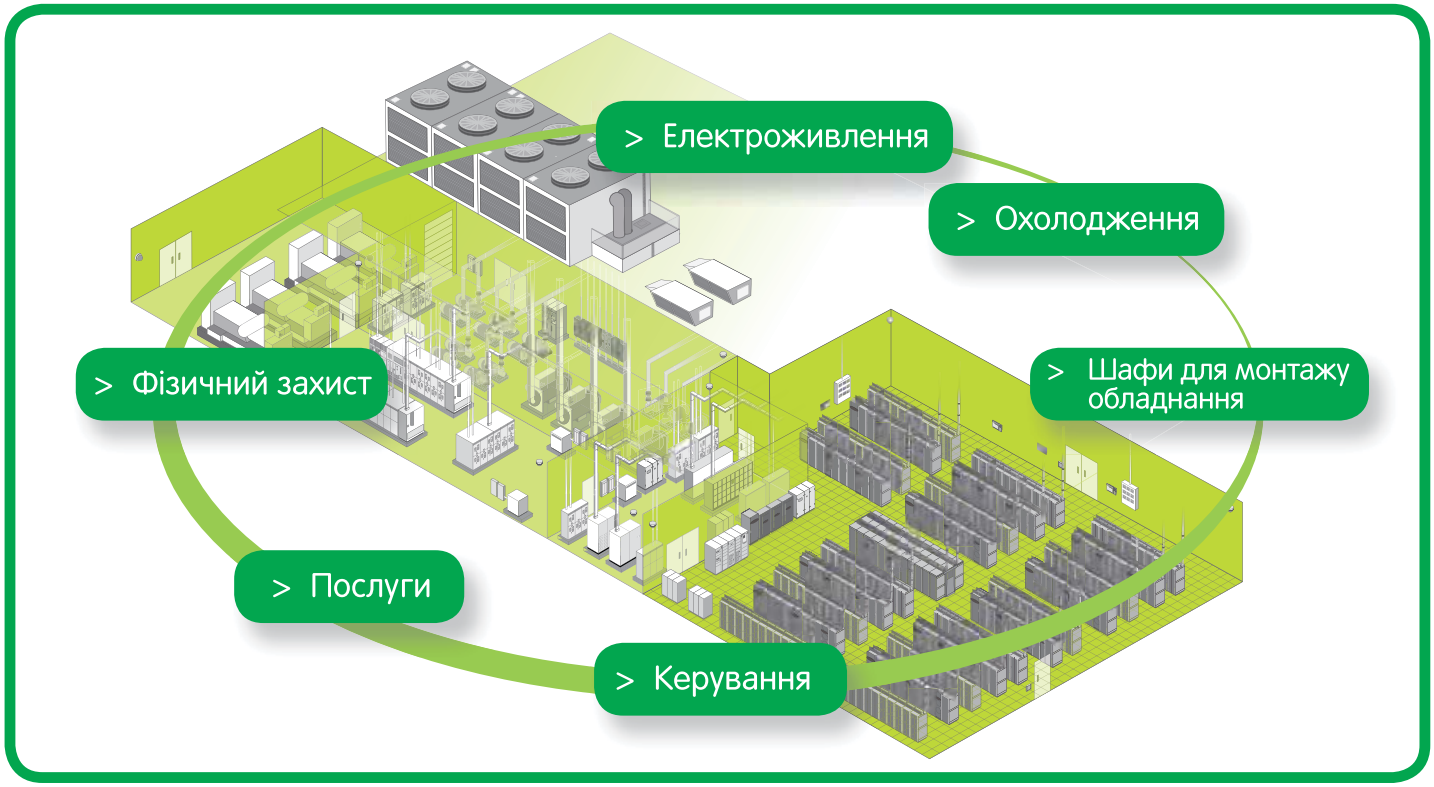
«Компьютерная преступность не имеет национальности и территориальной привязки, — отмечает Илья Сачков, генеральный директор Group-IB. — Российские хакеры давно и активно взаимодействуют с украинскими «коллегами». Поэтому и мы стараемся укрепить свои позиции и найти сильных партнеров.

«Наша компания максимально внимательно относится к вопросам безопасности, особенно в системах интернет-банкинга, ведь именно интернет-банкинг является наиболее «лакомым кусочком» для сетевых мошенников, — говорит Игорь Бабченко, директор компании CS. — Поэтому состоявшаяся встреча закономерна, а перспективность совместной работы двух компаний на почве защиты финансов в Интернете — несомненна. Совместная борьба с компьютерными преступлениями — залог безопасности наших клиентов в Интернете».

КОМПАНИИ И ОРГАНИЗАЦИИ В НОМЕРЕ

Amazon ... 20
AMD ... 4
ARM ... 20
Check Point Software Technologies ... 8
Cisco ... 8
CS ... 4
De Novo ... 8
Dell ... 20
DiaWest - Комп'ютерний світ ... 21
Epson ... 6
Forrester ... 20
Fortinet ... 8
Fujitsu Technology Solutions ... 20
Group-IB ... 4
IDC ... 3
Intel ... 10
McAfee ... 21
Microsoft ... 6, 10
MiroHost ... 21
Oracle ... 12
Ponemon Institute ... 14
ProNET ... 8
Quest Software ... 12
Symantec ... 8, 10, 11
Thales ... 14
Veeam Software ... 16
Zenoss ... 22
БАКОТЕК ... 12
БМС Консалтинг ... 8
Дробак ... 21
Инком ... 8, 13, 14
Комплексные решения ... 8
Лаборатория Касперского ... 3, 8, 16
HP ... 3, 16, 20
Укртрансгаз ... 12
Чумак ... 14

Як підвищити ефективність та готовність центру обробки даних?



Компанія Schneider Electric знає як!

Об'єднання інженерних систем на всіх рівнях

У світлі сучасних завдань в галузі IT Schneider Electric вважає необхідним розглядати центр обробки даних як повністю інтегровану систему — від шафи до ряду і від окремого приміщення до будівлі в цілому. Ми називаємо це інтеграцією інженерної інфраструктури центру обробки даних. До її складу входять системи електроживлення, охолодження, шафи для монтажу обладнання, системи забезпечення фізичного захисту. Моніторинг інженерної інфраструктури ЦОД та керування нею здійснюється за допомогою використання програмних продуктів та із залученням професійних послуг. Це єдиний вірний спосіб досягнення максимальної ефективності, економічності витрат енергії та постійної експлуатаційної готовності.

Ефективність та готовність інженерних систем

На сьогодні неможливо обійтися ні без максимальної ефективності використання енергії, ні без постійної експлуатаційної готовності. Для вирішення цього комплексного завдання слугує стратегія інтеграції систем охолодження Schneider Electric на всіх рівнях інженерної інфраструктури ЦОД. Цей комплексний підхід забезпечує справжню економію електроенергії — але не в якому разі не за рахунок готовності. Ми добиваємося подальшої оптимізації експлуатаційної готовності та ефективності завдяки інтегрованій програмній платформі, що забезпечує моніторинг всієї інженерної інфраструктури та керування нею. Це комплексне рішення забезпечує повноту інформації та взаємодії по всій інженерній інфраструктурі ЦОДу.

Об'єднання з найважливішими галузевими партнерами

Будівництво центру обробки даних передбачає постійний взаємозв'язок та координацію з постачальниками обладнання та іншими ключовими партнерами. Schneider Electric має у своєму розпорядженні унікальну мережу постачальників консультаційних та сервісних послуг, налагоджені стосунки та практичний досвід, що дозволяє компанії претендувати на роль єдиного постачальника всього необхідного для втілення ідеї інтегрованого центру обробки даних в реальність.

Архітектура ефективного керування енергією Active Energy Management

> **Електроживлення** Підсистема електроживлення поєднує все — від резервних генераторів до ДБЖ та систем розподілення живлення — із забезпеченням сумісності обладнання різних виробників.

> **Охолодження** Наші комплексні системи охолодження забезпечують максимальну ефективність та постійну експлуатаційну готовність, об'єднуючи чілери, периметричні та внутрішньорядні кондиціонери, системи ізоляції повітря в стояку та в «гарячому» коридорі.

> **Фізичний захист** Універсальна панель огляду дозволяє з одного робочого місця охопити контролем та відеоспостереженням одразу велику кількість об'єктів.

> **Серверні та телекомунікаційні шафи:** Шафи для монтажу IT-устаткування будь-яких виробників, додаткові пристосування та системи ізоляції повітряних потоків забезпечують все необхідне для роботи обладнання високої енергетичної щільності.

> **Послуги** Schneider Electric пропонує повний комплекс професійних послуг на етапах проектування, будівництва та експлуатації ЦОД.

> **Керування** Наша виняткова інтегрована архітектура програмного забезпечення дозволяє отримати повне уявлення про споживання енергії всіма інженерними системами ЦОДу, добитися ефективності її використання та постійної готовності систем.

Завантажте БЕЗКОШТОВНО будь-які інформаційні статті APC протягом 30 днів та станьте учасником розіграшу* – ВИГРАЙТЕ планшетний комп'ютер iPad 2!

Завітайте на сайт www.SEreply.com та введіть код 17655p
Тел.: +38 044 538-1478 • Факс: +38 044 538-1479

Schneider Electric™

©2012 Schneider Electric. всі права захищені. Бренди Schneider Electric, Active Energy Management та APC є власністю компанії Schneider Electric Industries SAS або її дочірніх компаній. Усі інші товарні знаки належать їхнім власникам. Інформація публікується на правах реклами. *З термінами та умовами проведення розіграшу ви можете ознайомитися на сайті www.apc.com/promo при заповненні реєстраційної форми.
APC by Schneider Electric, у Києві: 03057, Україна, Київ, вул. Металістів, 20 Т • Тел.: +38 044 538-1478, факс: +38 044 538-1479. Центр підтримки клієнтів: 0 800 502-7220, E-mail: apcukr@apc.com • 998-2599_UA_C

Pelican Publishing PCWEEK UKRAINIAN EDITION

Учредитель
«Пеликан Паблишинг»

Издатель
ООО «СК Украина»

Директор
НАТАЛЬЯ ПРОЦЕНКО

Директор по развитию бизнеса
ОЛЕСЯ БАБИЧ

Редакция

Над номером работали:
ОЛЕГ ПИЛИПЕНКО
ВЛАДИМИР ИЗМАЙЛОВ
СЕРГЕЙ ПЕТРЕНКО
ВАЛЕРИЯ НЕВСКАЯ

Литературный редактор
ЕЛЕНА СОЛОДОВНИК

Главный дизайнер
ЕЛЕНА ГАРБАР

Отдел рекламы

Тел./факс (044) 361-70-57
E-mail: press@skukraine.com
E-mail: sales@skukraine.com

Распространение

Тел./факс (044) 361-70-57

© «Пеликан Паблишинг», 2012

просп. Победы, 5,
01135, г. Киев

PCWeek/Ukrainian Edition. Газета печатается по лицензионному соглашению с компанией Ziff Davis Publishing Inc.
Перепечатка материалов допускается только с разрешения редакции. За содержание рекламных объявлений редакция ответственности не несет. Editorial items appearing in PCWeek/UE that were originally published in the U.S. edition of PCWeek are the copyright property of Ziff Davis Publishing Inc. Copyright 2012 Ziff Davis Inc. All rights reserved. PCWeek is trademark of Ziff Davis Publishing Holding Inc.
Газета зарегистрирована Государственным комитетом телевидения и радиовещания Украины.
Свидетельство о регистрации № 9892 от 27.05.05

Печать:
«Формула - I»
04136, г. Киев,
ул. М. Гречко, 13,
Тел./факс (044) 498-39-30

PCWeek/UE выходит один раз в две недели. Распространяется по подписке.

Тираж 10 000 экземпляров

«ФАБРИКА ПЕЧАТИ» НА НОВЫЙ ЛАД

ОЛЕГ ПИЛИПЕНКО

Чтобы преуспеть на высококонкурентном рынке печатных устройств, необходимо постоянно находить новые технологические решения. Epson — одна из тех компаний, которая успешно решает эту задачу. В сегменте струйных принтеров японский производитель является одним из наиболее заметных игроков и, без преувеличения, новатором. Компания постоянно повышает «скорострельность» своих устройств, одновременно снижая себестоимость печати. Фактически струйная печать в исполнении Epson становится все более качественной и экономичной и, благодаря таким характеристикам, претендует на те области применения, в которых сейчас доминируют «лазерники».

В конце лета компания представила в Москве обновленный модельный ряд своих продуктов для бизнеса. Новшества появились практически во всех линейках оборудования, но наиболее интересные продукты — именно в категории струйных принтеров. Веховой разработкой производителя в этом сегменте стала линейка устройств под названием «Фабрика печати Epson», впервые анонсированная около года назад (см. PCWeek/UE № 14-15, 2011).

Напомним, что принтеры линейки «Фабрика печати Epson» отличаются новой «безкартриджной» конструкцией: оригинальные чернила Epson заправляются во встроенные емкости из контейнеров по 70 мл. Благодаря такой конструкции обеспечивается чрезвычайно низкая стоимость печати, при этом пьезоэлектрическая технология печати Epson Micro Piezo гарантирует высочайшее качество. Особый дизайн контейнеров делает процедуру перезаправки простой даже для неопытного пользователя.

Еще в прошлом году компания вывела на рынок модели L100 (офисный принтер), L200 (офисное МФУ) и L800 (шестицветный фотопринтер). Теперь «фабричная» линейка пополнилась сразу пятью новинками — принтерами Epson L110 и L300, МФУ Epson L210, L355 и L550. В этих устройствах усовершенствован алгоритм печати и доработана формула чернил, благодаря чему «выстреливаемая» капля уменьшилась в размере. Таким образом, принтеры стали еще более экономичными. Себестоимость печати на новых устройствах серии составляет всего 1 копейку за страницу для монохромной печати и 2-3 копейки для цветного документа формата А4. Это примерно на 20% ниже, чем у линейки 2011 г.

Модели L110 и L210 пришли на смену устройствам L100 и L200 соответственно. При перезаправке чернил в новинках не нужно вводить ID-код, поэтому емкости пополняются быстро и легко. Кроме того, продукты на 10% компактнее своих предшественников.

Цветной принтер Epson L300 и многофункциональное устройство Epson L355 имеют компактные размеры и обладают быстродействием до 33 стр./мин., а также возможностью печати и сканирования по Wi-Fi и с мобильных устройств.

Epson L550 был разработан специально для работы в малых и средних офисах. Устройство оснащено двустрочным ЖК-дисплеем, автоподатчиком оригиналов для сканеров и факсом при отправке документов. По скорости печати (до 33 стр./мин.) данная модель не уступает лазерным принтерам. Epson L550 оснащен портом Ethernet для работы с несколькими ПК по сети, также все аппараты имеют порт USB 2.0.

МФУ L355 и L550 поддерживают функцию Epson iPrint для печати и сканирования с мобильных устройств на базе iOS и Android. Все новые устройства серии «Фабрика печати Epson» совместимы с наиболее популярными операционными системами PC и Mac OS. Epson предоставляет на L110 и L210 гарантию 12 мес. или 15 тыс. отпечатков, а на L300, L355 и L550 — 12 мес. или 30 тыс. отпечатков. Цены на новинки пока не объявлены.

МФУ Epson L355 обладают скоростью печати до 33 стр./мин., а также возможностью управления по Wi-Fi и с мобильных устройств

Благодаря приложению Epson iProjection можно легко передавать изображение и управлять проектором с мобильных устройств Apple

«Полку» проекторов прибыло

Epson традиционно занимает первое место на рынке проекторов в СНГ. С целью укрепления лидерских позиций компания обновила линейки своих бизнес-проекторов, представив ряд новых устройств. Ультрапортативные проекторы EB-1751/1761W/1771W/1776W ориентированы на мобильных пользователей. Устройства новой серии сочетают в себе яркость и высокое качество изображения, малый вес и компактный дизайн — это пока самые легкие и тонкие проекторы Epson. Толщина корпуса моделей всего 4,4 см, а масса 1,6 кг. Производитель заявляет, что они отличаются быстрой и простой настройкой, а также функциями моментального включения и выключения. С расстояния 1,35 м такие устройства формируют картинку диагональю до 60 дюймов.

Множество дополнительных функций в серии Epson EB-1761W/1771W/1776W значительно расширяют возможности работы. Например, Multiscreen служит для подключения до четырех проекторов к одному компьютеру, а Split Screen позволит просматривать на одном экране два изображения с разных источников. Для беспроводного соединения в проектор необходимо установить модуль беспроводной сети ELPAP07, который продается отдельно для моделей EB-1761W/1771W, а с EB-1776W поставляется в комплекте.

С помощью нового приложения Epson iProjection можно легко передавать изображение и управлять проектором с мобильных устройств Apple. Приложение поддерживает все основные форматы (World, Excel, PowerPoint, Keynote, PDF) и позволяет демонстрировать фотографии в JPG- и PNG-форматах.

Скоростные сканеры

Компания Epson также представила новые линейки планшетных сканеров форматов А3 и А4. Серия WorkForce DS-5500/6500/7500 — планшетные сканеры А4 с базовым функционалом и высокой дневной нагрузкой. Они предназначены для таких сфер, как образование, медицина, государственный сектор и т.д.

Продукты Epson WorkForce DS-6500/6500N оснащены устройством автоматической подачи документов емкостью 100 листов. Особенность этих сканеров — два модуля для сканирования документов сразу с обеих сторон за один проход. Кроме того, модели оснащены ультразвуковым сенсором двойного захвата, что помогает избежать попадания в автоподатчик скрепленных или склеенных документов. Сканеры Epson WorkForce DS-6500/6500N могут оцифровывать документы со скоростью до 25 стр./мин. или 50 изображений/мин., а максимальный ресурс составляет 3 тыс. страниц в день.

Серия WorkForce DS-7500/7500N обеспечивает еще более высокую скорость сканирования — 40 стр./мин. или 80 изображений/мин., а максимальная дневная нагрузка достигает 4 тыс. страниц. Все сканеры обновленной серии Epson WorkForce DS-5500/6500/7500, а также их сетевые версии поддерживают новый формат сжатия HW JPEG Compression.

Серия WorkForce DS-50000/60000/70000 — это высокопроизводительные сканеры формата А3. Каждый аппарат поставляется в двух версиях: базовой с локальным подключением по USB и сетевой. Устройства серии Epson WorkForce DS-70000/70000N оснащены автоподатчиком на 200 листов с возможностью автоматического двустороннего сканирования за один проход листа. Модели отличаются высокой скоростью (70 стр./мин. или 140 изображений/мин.) и значительным ресурсом (до 8 тыс. сканирований в день). Новые сканеры нацелены на банковский сегмент, государственные учреждения, сферу образования, организации малого и среднего бизнеса.

Сканеры Epson WorkForce DS-60000/60000N позволяют сканировать документы со скоростью до 40 стр./мин. или 80 изображений/мин., максимальная нагрузка в день составляет 5 тыс. сканирований. Также они оснащены ультразвуковым сенсором для определения двойной подачи листа и автоподатчиком для облегчения работы с большими объемами документов.

Инновационная технология Epson ReadyScan LED применяется во всех сканерах обновленной линейки, что дает существенную экономию времени на прогрев устройства

Модели Epson WorkForce DS-50000/50000N — самые доступные по стоимости устройства в линейке сканеров Epson формата А3 с базовыми функциональными возможностями.

Все новые сканеры поддерживают специализированное программное обеспечение Epson Document Capture Pro. С его помощью можно сортировать документы при потоковом сканировании, а также сканировать информацию в облачное хранилище данных.

Инновационная технология Epson ReadyScan LED применяется во всех сканерах обновленной линейки, что дает существенную экономию времени на прогрев устройства. Таким образом, сразу после включения все сканеры готовы к работе.

При использовании материалов ссылка на сайт pcweek.ua обязательна

КОМПЛЕКСНЫЕ РЕШЕНИЯ

ДЛЯ ПОСТРОЕНИЯ СИСТЕМ
ВИДЕОНАБЛЮДЕНИЯ И КОНТРОЛЯ ДОСТУПА

Системы видеонаблюдения

Программное обеспечение для систем видеонаблюдения

Физический контроль доступа

Системы IP-взаимодействия и сотрудничества

МЕГАТРЕЙД
СПЕЦІАЛІЗОВАНИЙ IT-ДИСТРИБУТОР

Официальный дистрибутор **Cisco** в Украине

Бизнес-центр «Grand Step», ул. Полевая, 24 Д, Киев, 03056, Украина
тел.: +380 44 538 00 06, факс: +380 44 538 00 16
e-mail: office@megatrade.ua, www.megatrade.ua

Welcome to
the Human Network

CISCO

ЗАЩИТА ДАННЫХ: ОБЪЕМНЫЙ ВЗГЛЯД

ЭКСПЕРТИЗА

Информационная безопасность давно вышла на первые места в списке приоритетов ИТ-служб компаний и организаций всего мира и покинет топлист не скоро: изощренность и количество угроз растут из года в год. Почти каждую секунду создаётся новый образец вредоносного ПО, каждый день по всему миру происходят тысячи атак на информационные ресурсы… Неудивительно, что индустрия технологий и решений в области ИБ давно перестала быть нишевой и демонстрирует стремительный рост.

Согласно прогнозу Gartner, в 2012 г. мировые расходы на информационную безопасность вырастут на 8,4% и продолжат расти до 2016-го. Ожидается, что в 2012 г. они составят 60 млрд долл. против 55 млрд долл. год назад, а к 2016 г. вырастут до 86 млрд долл. Таким образом, среднегодовой темп прироста рынка услуг управления ИБ за пятилетний прогнозный период составит 16,8%.

Главными причинами увеличения бюджетов на ИБ названы постоянно растущие угрозы и всё большая прицельность и сложность атак. Gartner ожидает, что организации будут стремиться внедрять всё более надежные и адаптивные решения, чтобы уменьшить уязвимость и упредить возможный будущий риск.

Технологии и услуги ИБ должны получить ускорение ввиду растущей активности преступности, проистекающей из трудной экономической ситуации. Эта тенденция противоположна тому, что будет наблюдаться на других рынках, указывают аналитики Gartner.

Самыми быстрорастущими сегментами этого рынка станут управляемые услуги ИБ, устройства-шлюзы, а также управление информационной безопасностью и событиями (SIEM). В сегменте облачных услуг ИБ будет наблюдаться рост выше среднего.

Услуги управления безопасностью особенно востребованы, полагают в Gartner. Корпоративные заказчики большей частью внедрили технологии ИБ и уже обеспечили соблюдение регулятивных норм. Поэтому атакующие теперь берут прицел ниже, на мелкие компании и средний сегмент, где могут рассчитывать на больший успех. Это заставит многие мелкие фирмы, которые не имеют большого бюджета, прибегнуть к аутсорсингу услуг ИБ.

ТРЕНДЫ РЫНКА

Если в начале века вопросы безопасности по большей части являлись внутренним делом бизнеса, то сегодня это не столько правила хорошего тона, сколько законодательное требование. «Масла в огонь подливает» и закон о персональных данных, к реализации положений которого компании всё-таки вынуждены были приступить.

Чтобы более подробно узнать о тенденциях на рынке информационной безопасности в Украине, PCWeek/UE пригласил к участию в подготовке темы номера крупнейших вендоров и системных интеграторов. В частности, мы попросили игроков оценить изменение бюджетов, выделяемых на ИБ, предпочтения заказчиков и описать предлагаемые на рынке продукты и технологии для защиты от онлайн-мошенничества и работы в виртуальных средах.

По вашим оценкам, как изменились ИТ-бюджеты заказчиков, выделяемые на ИБ?

Владимир Илибман: Бюджеты на ИБ у клиентов связаны с общим бюджетом компании на ИТ. Из нашего опыта они составляют от 5 до 10% от общего бюджета информационных технологий. Затраты на безопасность растут даже несколько быстрее, чем общий бюджет ИТ в организации.

Андрей Божок: На текущий момент бюджеты на ИБ выделяются только в случае, если нужно закрыть критические уязвимости. Дорогие решения в этом сегменте такая же редкость, как и, например, строительство ЦОДов. По сравнению с 2006-м или 2007-м мы отмечаем прирост на уровне 20%.

Владимир Стыран: На самом деле вопрос не совсем корректен, так как бюджет на безопасность компании после достижения ею определенного уровня зрелости перестает иметь к ИТ прямое отношение. Компании, которые уже поняли, что ИБ и ИТ являются различными, порой несовместимыми, областями деятельности, с одной стороны, увеличивают бюджет на информационную безопасность, а с другой — начинают использовать его более эффективно.

В целом в течение 2011-2012 гг. мы наблюдаем стабильный рост бюджетов, выделяемых на защиту корпоративной информации и, как следствие, позитивную динамику рынка средств и услуг ИБ.

Василий Задворный: На сегодня законодательные требования не являются основным двигателем развития ИБ. Если говорить про закон о защите персональных данных, то в большинстве своем малый и крупный бизнес ограничиваются выполнением требований по регистрации баз персональных данных. Компании финансовой сферы еще могут разрабатывать нормативную документацию, которая регулирует внутреннюю деятельность в контексте закона. В части применения технических средств защиты: либо используют то же, что и для всей ИТ-инфраструктуры, либо ничего. Если говорить о регулировании НБУ, то поведение банков неоднозначно. Одни пытаются решить проблему лишь написанием регламентной документации, а другие осознают необходимость полноценной СУИБ: выделяют бюджеты и полноценно выстраивают процессы управления, то есть создают действительно работающую Систему управления информационной безопасностью.

Владимир Удалов: Как показало исследование «Лаборатории Касперского» об основных проблемах и тенденциях в сфере ИТ-безопасности корпоративного сектора Украины, в бизнес-среде хорошо осведомлены об основных киберугрозах, однако инвестиции в ИТ ниже среднемировых показателей. Так, лишь 35% украинских компаний считают существующий уровень инвестиций в ИТ-безопасность достаточным. В мире этот показатель равен 55%. Большинство респондентов, которые недовольны финансированием, охотно бы увеличили объем инвестиций на 25% и более.

Также хотелось бы отметить, что 69% представителей украинских компаний полагают, что в их организациях недостаточно не только финансовых ресурсов, но и специалистов, знаний и системных ресурсов.

Александр Стафоркин: В последнее время в общем бюджете предприятий появилась статья расходов на ИБ. Но, к сожалению, — только у банков и части государственных предприятий.

Коммерческие структуры в основном выделяют бюджет на ИБ по остаточному принципу. Поэтому с ситуацией «Зачем мне DLP, если на эти деньги я могу купить новый трактор…» приходится сталкиваться до сих пор.

В какие сегменты ИБ заказчики наиболее активно инвестируют сегодня, в связи с вышеупомянутыми законодательными изменениями? Какие тренды вы можете отметить в предпочтениях заказчиков?

Владимир Илибман: Клиенты по-прежнему больше инвестируют в программные и аппаратные продукты для защиты сети, рабочих станций и ЦОДов. Но при этом выросла доля ИБ-консалтинговых услуг по построению систем управления информационной безопасностью (СУИБ), компании разрабатывают внутренние нормативные базы и процессы для соответствия требованиям НБУ и закону по защите персональных данных. Для многих банков также актуальной статьей расходов является процедура сертификации по требованиям PCI DSS.

Владимир Стыран: Заказчики в который раз задумались о наведении порядка в ИБ, а это скорее не вложения в конкретные ИТ-решения, а выстраивание процессов и организационные изменения. Причем меняется не только организационная структура, но и общая культура бизнеса. Компании начинают задумываться о том, что они защищают, с какой целью, а главное — чья это задача. Таким образом, мы можем наблюдать спрос на консалтинг по ИБ, поскольку так быстрее, а иногда и дешевле, выстроить бизнес-процессы безопасности. А вложения в ИТ-решения становятся вторичными и происходят осознанно и эффективно — через оценку рисков и доказательство бизнес-потребности и экономической целесообразности высшему руководству.

Учитывая вышесказанное, наибольший интерес среди украинских компаний вызывают проекты по оценке и повышению уровня защищенности компании и выстраиванию процессов ИБ.

Владимир Удалов: Наиболее востребованы сейчас комплексные системы класса endpoint security, которые заменяют «зоопарк» из разнородных нишевых продуктов от разных производителей. При этом они обладают единой централизованной системой управления. Современные продукты endpoint security, помимо привычных всем модулей антивирусной защиты и файрвола, включают в себя мощный функционал по контролю запускаемых приложений, веб-контроль, контроль устройств и контентную фильтрацию. Собранные вместе, все эти модули заметно повышают уровень информационной безопасности на предприятии. Но самое важное — они позволяют регламентировать и контролировать использование сотрудниками персональных компьютеров, определяя перечень разрешенных к запуску программ, контролируя посещение веб-ресурсов и подключение внешних устройств, например USB-флешек.

Часто ли интерес заказчиков выходит за пределы базового функционала по ИБ (антивирус, файрвол)? Интересуются ли они решениями IPS, UTM, DLP и другими?

Антон Разумов: С каждым годом растет количество угроз, подстерегающих пользователей Интернета во всем мире. Компании все лучше это понимают и стремятся защитить себя. Речь идет не только о непосредственных угрозах, но и о контроле использования интернет-ресурсов. Например, в последнее время участились запросы на решения, позволяющие блокировать использование торрентов, Skype, ограничивать просмотр роликов с YouTube. Ну а стандартные UTM-функции, такие как IPS, антивирусные проверки на шлюзе, фактически стали стандартными.

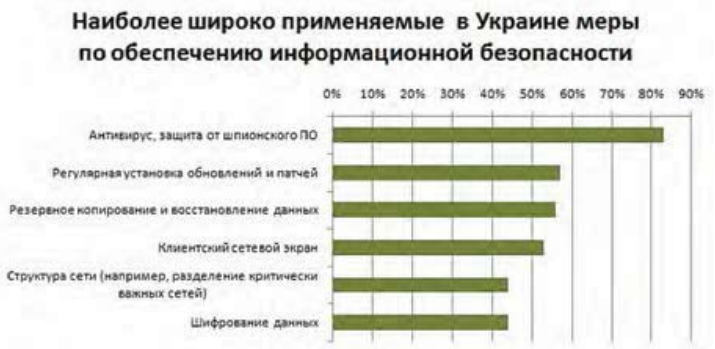
Владимир Илибман: На сегодня многие компании уже внедрили базовые меры для защиты сети. Например, внедрена защита внешних периметров с помощью базовых файрволов, рабочие станции и сервера оснащены антивирусными программами. Поэтому сейчас корпоративные заказчики интересуются расширенным функционалом защиты. Для защиты внешнего периметра заказчики все чаще используют межсетевые экраны следующего поколения (Next Generation FW), которые обеспечивают глубокий анализ и защиту интернет-приложений, но при этом позволяют привязывать политики доступа к ролям сотрудников. Актуальным является контроль доступа изнутри сети. Фактически эта ниша на рынке свободна — менее 10% компаний ограничивают доступ в проводную и беспроводную сеть организации изнутри. Соответственно есть интерес к решениям класса Network Admission Control. В последние годы активно привлекает внимание защита центров обработки данных. В организациях накапливаются огромные объемы электронных данных, которые нужно обрабатывать, хранить и, разумеется, защищать. ЦОДы выдвигают повышенные требования к системам защиты, связанные со скоростью работы, надежностью и интеграцией в инфраструктуру ЦОДа.

Андрей Божок: Спрос рождает предложения. Заказчики очень активно интересуются различными решениями. На данный момент даже обычные антивирусы вышли из базового функционала и предлагают дополнительные возможности, как и файрволы. В каждом решении уже есть дополнительные возможности. Интерес к различным решениям достаточно высокий, постоянно происходят какие-то нововведения. Новые уязвимости и требования регулирующих органов повышают интерес заказчиков.

Василий Задворный: Решениями базовой защиты рынок насытился пару лет назад. Сейчас большее развитие получают направления SIEM, IDM, DLP, DAM, GRC.

Александр Стафоркин: Отвечая на требования соответствия определенным стандартам (ISO 27001), клиенты все больше обращают внимание на SIEM- и DLP-системы. Коммерческие клиенты начали интересоваться шифрованием дисков ноутбуков.

Известно, что обмен шифрованными данными по сети в некоторых случаях приводит к значительному снижению производитель-



Источник: «Лаборатория Касперского»

ности приложений. Часто ли вы встречались с применением шифрования данных у своих заказчиков? Что останавливает клиентов, кроме возможной потери производительности, и что стимулирует их к применению криптографии?

Владимир Илибман: Необходимость использования криптографии вызвана двумя причинами. Во-первых, это регуляторные требования по защите чувствительной и конфиденциальной информации (персональной информации, карточной информации в случае PCI DSS). Во-вторых, это осознание компанией реальных рисков, связанных с передачей конфиденциальной информации по незащищенным каналам — в первую очередь через Интернет и арендованные внешние каналы. В последнее время требования к скорости шифрования существенно выросли. Существуют заказчики, которые желают шифровать многогигабитные каналы связи между площадками и ЦОДами. К счастью, сейчас существуют технологии, которые обеспечивают аппаратное высокоскоростное (1Гбит/с и 10Гбит/с) шифрование без влияния на производительность сети и приложений. Кроме стандартного шифрования по протоколу IPSec, появилась альтернатива шифрования на уровне Ethernet — технология MacSec (стандарт 802.1AE). Еще одним вопросом со стороны заказчика является легальность используемого шифрования и сертификация в Украине. Для ответа на данный вопрос Cisco совместно с украинскими разработчиками выпустила несколько программно-аппаратных криптошлюзов, которые обеспечивают шифрование по украинским государственным стандартам и прошли сертификацию Госспецсвязи.

Андрей Божок: Обмен шифрованными данными не так сильно снижает производительность, как это представляют себе заказчики. Их останавливает отсутствие дополнительной информации по шифрованию. В Украине не так много компаний, у которых есть хорошие специалисты по криптографии: тут большую роль играет слабая компетенция в этой области. А главным стимулом к шифрованию информации является сохранность своих конфиденциальных данных. Если данные зашифрованы, получить к ним доступ очень проблематично, особенно если все реализовано на программно-аппаратном уровне.

Владимир Стыран: Утверждение, что обмен шифрованными данными приводит к значительному снижению производительности приложений, потеряло актуальность около пяти лет назад. Ведь за последние годы криптографические алгоритмы не изменились: AES был стандартизирован в 2002 г., RSA — еще в далеком 1977-м. По закону Мура, вычислительные мощности удваиваются каждые два года, так что на сегодняшний день с криптографией не справляются только очень ветхие или очень неправильно спроектированные системы. Добавьте к этому повсеместную аппаратную поддержку функций блочного шифрования в современных процессорах, и вы поймете, что помешать использованию криптографии теперь может только нежелание ее использовать.

Василий Задворный: Сегодня не составляет особых проблем обеспечить защищенный канал без ощутимых потерь в скорости при шифровании на сетевом уровне. А вот в области шифрования приложений все зависит от архитектуры информационной системы и применяемых технологий. Основными двигателями к применению средств обеспечения ИБ являются: произошедшие инциденты и внешнее регулирование (государственное, международное, материнской компании). Новые системы все чаще проектируют, учитывая необходимость шифрования, старые же действительно могут содержать архитектурные ограничения и, как следствие, — приводить к резкому снижению производительности. В связи с этим систему оставляют уязвимой.

Владимир Удалов: Тип передаваемых по сети данных (шифрованные или нешифрованные) никак не влияет на скорость передачи. Сам модуль шифрования, занимающийся шифрованием и дешифровкой данных, также не оказывает сколь-нибудь заметного влияния на производительность компьютера.

Главным стимулом для внедрения шифрования является повышенная мобильность сотрудников — они часто работают дома, используя корпоративный ноутбук, и ездят в командировки. Современные программные решения дают возможность из любой точки мира получить доступ к корпоративной почте, корпоративным информационным порталам. Это, безусловно, повышает производительность сотрудников, позволяет им быть на связи практически круглосуточно.

Но при этом конфиденциальная корпоративная информация, свободно перемещаемая сотрудником на ноутбуке, подвергается риску утери и компрометации. А когда в крупной компании каждый второй сотрудник регулярно работает из дома, потеря ноутбука перестает быть из ряда вон выходящим событием, и становится своеобразной рутиной для ИТ-отдела. И вот тут-то и возникает вопрос — как защитить конфиденциальные данные, хранящиеся на ноутбуке. Шифрование является одним из инструментов, применяемых для решения этой задачи, наряду с использованием надежной системы класса endpoint security.

Онлайн-платежи

Согласно прогнозам IDC в 2012 г. будет совершено более 1 млрд онлайн-покупок на общую сумму более 1,2 трлн долл. В сложившихся условиях рост онлайн-платежей сопровождается повышением активности мошенников, а пользователи все чаще переживают за сохранность своих данных. Согласно опросу «Лаборатории Касперского», кража финансовой информации всерьез беспокоит 40% опрошенных, а 21% считает ее хищение наиболее серьезной угрозой.

Редакция PCWeek/UE поинтересовалась у экспертов, какие продукты и технологии в области защиты онлайн-платежей они предлагают и есть ли интерес к подобного рода решениям со стороны заказчиков?

Антон Разумов: Пожалуй, наиболее эффективным способом для защиты от мошенников является использование одноразовых кодов. Причем не обязательно снабжать каждого пользователя дорогостоящим устройством — очень высокого уровня безопасности можно достичь при помощи отправки SMS на его телефон. Важное достоинство этого подхода состоит в том, что ответственность за работоспособность такого устройства лежит на пользователе, и это позволяет обойтись без специальной службы. Например, в случае утери телефона сам пользователь озаботится его заменой и восстановлением SIM-карты.

В решении Check Point Mobile Access Blade предусмотрена возможность задействовать дополнительную авторизацию с помощью SMS-сообщения, т.е. пользователь авторизуется обычным образом (вводя имя и пароль) после чего ему предлагается ввести одноразовый код, полученный по SMS. Систему можно настроить таким образом, что при отказе пользователя ввести этот код, доступ будет ограничен, например, только для просмотра остатков по счетам, но не для переводов. Причем данный функционал настраивается на шлюзе безопасности, что значительно облегчает сопровождение самой банковской системы.

Еще более продвинутым решением для онлайн-платежей является специализированное устройство Check Point GO. Внешне это обычная флешка, которую удобно носить с собой. Но при подключении к любому компьютеру с Windows после ввода специального пароля запускается безопасная среда, изолированная от основной операционной системы, из которой, в свою очередь, устанавливается защищенное соединение в банк. Таким образом, пользователь может безопасно совершать банковские операции даже с чужих компьютеров.

Владимир Илибман: В мировой практике защита систем электронных платежей осуществляется в соответствии со стандартами платежных систем Visa/Mastercard — Payment Card Industry Data Security Standard (PCI DSS). Cisco совместно с партнерами — компаниями EMC/RSA и HyTrust — разработала референс-архитектуру решения для PCI DSS. Архитектура была оценена независимым аудитором Verizon Business. Блоки данной архитектуры могут использоваться банками, традиционными и интернет-магазинами для защиты своих информационных систем.

Интерес к решению для защиты онлайн-платежей демонстрируют в первую очередь банки со своей системой процессинга платежей. Именно они находятся под пристальным вниманием платежных систем, и отсутствие соответствующей защиты может повлечь предупреждения, штрафы и даже отключения со стороны Visa/Mastercard. Интернет-магазины и небольшие банки зачастую перекладывают защиту интернет-платежей на вышестоящие процессинговые центры и провайдеров платежных систем, через которые осуществляется обработка транзакций. То, чем реально интересуются все категории заказчиков, — это системы защиты от DDoS-атак. В Украине, как и в России, DDoS-атаки становятся дешевым и доступным элементов конкуренции, которым подвергаются и сайты онлайн-торговли.

Илья Магась: Для того чтобы используемые технологии онлайн-платежей были максимально защищены от компрометации данных транзакции и мошенничества, банку следует решить несколько задач. Во-первых, необходима надежная аутентификация клиента и транзакции, которая не даст мошеннику провести операцию, перехватив пароль к сайту веб-банкинга. Во-вторых, должно использоваться надежное шифрование канала связи и подтверждение аутентичности сервера. Это позволит минимизировать опасность фишинговых атак на наиболее доверчивых клиентов банка. В-третьих, не обойтись без системы мониторинга операций. Она своевременно выявит подозрительные действия клиентов, заблокирует потенциально опасные операции и уведомит подразделение банка, отвечающее за борьбу с мошенниками. «БМС Консалтинг» предлагает решения для двухфакторной аутентификации от ведущих производителей SafeNet, RSA. Также в нашем портфеле продуктов есть решения по мониторингу и корреляции событий и защите каналов связи от таких производителей, как Cisco, CheckPoint, Fortinet.

В связи с массовым переходом банков на дистанционное обслуживание наибольший интерес естественно мы наблюдаем с их стороны. Но также подобные решения остаются достаточно востребованными и в других крупных

ПРОДОЛЖЕНИЕ НА С.11>>>

НАШИ ЭКСПЕРТЫ

АНТОН РАЗУМОВ
Руководитель группы консультантов по безопасности Check Point Software Technologies Ltd

ВЛАДИМИР ИЛИБМАН
Технический консультант Cisco

АНДРЕЙ БОЖОК
Пресейл-менеджер компании ProNET

ВЛАДИМИР СТЫРАН
Ведущий консультант департамента консалтинга в области информационной безопасности ООО «БМС Консалтинг»

ВАСИЛИЙ ЗАДВОРНЫЙ
Руководитель отдела ИТ-консалтинга компании Инком

ВЛАДИМИР УДАЛОВ
Руководитель направления корпоративных продуктов в странах развивающихся рынков «Лаборатории Касперского»

АЛЕКСАНДР СТАФОРКИН
Менеджер по продажам решений в отрасли безопасности компании-интегратора «Комплексные решения»

ИЛЬЯ МАГАСЬ
Консультант службы телеком-технологий и информационной безопасности ООО «БМС консалтинг»

ГЕННАДИЙ КАРПОВ
Директор по технологиям De Novo

МИРОСЛАВ МИЩЕНКО
Эккаунт-менеджер Fortinet в Украине

ОЛЕГ ПРОСВЕТОВ
Технический консультант Symantec

При использовании материалов ссылка на сайт pcweek.ua обязательна

ОГРАДИТЬСЯ ОТ ИНСАЙДЕРОВ

ИНТЕРВЬЮ

ОЛЕГ ПИЛИПЕНКО

Традиционно считается, что DLP-системы в первую очередь предназначены для крупных корпораций. Однако Александр Суязов, консультант по информационной безопасности компании Symantec в России и СНГ, уверен, что именно СМБ-сегмент более всего нуждается в защите конфиденциальной информации.

PCWeek/UE: Когда в регионе СНГ стартовали первые проекты по внедрению DLP-систем? Какие компании проявляют к ним интерес?

АЛЕКСАНДР СУЯЗОВ: Направление DLP-решений достаточно молодое, продукты в этой области появились всего десять лет назад. Но когда на рынке возникает новое решение, заказчикам необходимо разъяснять его преимущества. Пока рынок зрел — прошло несколько лет. Поэтому первые проекты в СНГ мы реализовали 4-5 лет назад. Заказчиками были представительства западных компаний, так как в США и Европе DLP-системы уже лет восемь являются корпоративным стандартом. Одна из причин этого — законодательно прописанное требование сообщать об утечках всем клиентам, которые могут от этого потенциально пострадать. По сути, если в банке случилась утечка, он должен оповестить всех своих клиентов. Подобные корпоративные стандарты транслируются на все филиалы, включая представительства в других странах.

Облачная система закрывает только небольшую часть утечек, но ведь еще остаются рабочие станции, которые в любом случае необходимо защищать

Традиционно компания Ponemon Institute каждый год публикует отчет о стоимости утечек «Cost of a Data Breach». Последние пять лет удельная стоимость одной утечки в отношении пострадавшей от нее персоны колеблется на уровне 200 долл. Поэтому сегодня DLP-системы выбирают компании, обязанные законодательно защищать информацию, а также те, которые реально оценивают стоимость утечек.

PCWeek/UE: Многие заказчики полагают, что DLP-системы стоят слишком дорого для того, чтобы себя окупать. Насколько вы согласны с таким утверждением?

А.С.: DLP-решение способно предотвращать утечки, а значит, помочь компании сохранить свои средства. Поэтому для каждого заказчика окупаемость DLP-системы индивидуальна. Иногда всего одна утечка конфиденциальных данных может окупить внедрение DLP-системы. Особенно, если такая утечка будет стоить компании места на рынке. На этом фоне довольно странно наблюдать желание заказчика приобретать DLP-систему без функций блокирования утечек. Ведь в этом случае он покупает для себя просто решение для констатации факта утечки и совершенно не инвестирует средства в свою защиту.

Тем не менее, всегда есть возможность снизить затраты. Например, Symantec предлагает внедрять только часть модулей комплексного DLP-решения, которые максимально снизят риски, но при этом будут вполне приемлемы по цене для

Александр Суязов

конкретного клиента. В любом случае, стоимость решения должна быть сравнима с ценностью корпоративной информации. В противном случае внедрение защиты от утечек не оправданно.

Отмечу также, что с моей точки зрения, ущерб от утечек в СМБ выше, чем в больших организациях. Малые компании очень зависят либо от крупного клиента, либо от одной масштабной сделки... Любой «слив» критически важных сведений, который приведет к потере ключевого клиента или срыву контракта, может стать существенным ударом для бизнеса. В то же время в крупных корпорациях бизнес диверсифицирован, клиентов достаточно много. Потеря одного из них неприятна, но не смертельна.

Поэтому сегодня внедрение DLP-решений в СМБ-сегменте, на мой взгляд, является трендом. Этот бизнес начинает больше интересоваться DLP-системами, активно выбирает продукты.

PCWeek/UE: Насколько DLP-решения для малого бизнеса, выпускаемые Symantec, отличаются от решений для крупных корпораций?

А.С.: Комплексная DLP-система для небольших компаний может оказаться слишком «тяжелым» приобретением. В этом случае мы предлагаем внедрить только некоторые, наиболее важные модули. Например, заказчик может ограничиться лишь защитой рабочих станций, оставив на будущее другие модули. По сути это такие же технологии защиты, что и у крупных компаний, только с меньшим набором функций. Но и подобное решение способно справиться со своей задачей.

Стоит отметить, что в крупных корпорациях отделу информационной безопасности приходится решать более широкий спектр задач в области хранения данных. Ведь если в компании работает всего 10-20 человек, то обычно все сотрудники в курсе дел предприятия, нет строгого разделения ролей и корпоративных секретов. А в крупной организации каждая бизнес-единица нацелена на решение своих проблем. Должно быть строгое разграничение доступа к данным. Поэтому одна из важнейших задач в большой организации — правильное хранение информации и защита от утечек внутри компании.

PCWeek/UE: Много клиентов уверено, что настраивать и использовать DLP-систему слишком сложно из-за большого количества компонентов и различных параметров. Что предлагает в этом отношении Symantec?

А.С.: То, что DLP-система сложна в настройке, — это естественно. Она «привязывается» к бизнес-процессам и обороту информации внутри компании. Любое внедрение DLP предполагает, что все эти процессы в компании уже есть и формализованы или работа по их формализации начата. Может показаться странным, но DLP-система способна помочь в формализации и описании этих процессов.

С другой стороны мы стараемся предложить инструменты для упрощения и автоматизации настройки системы. Это и цифровые отпечатки, и самообучение системы. Мы предлагаем отказываться от трудоемких методов, например таких, как составление словарей. Ведь именно эти методы дают наибольшее количество ложных срабатываний и формируют негативное впечатление о системе в целом.

Обладая большим опытом внедрения DLP-систем, компания Symantec предлагает свою методологию, которая зачастую упрощает старт проекта. Этой методологии мы обучаем своих партнеров, хотя можем научить и заказчиков. У нас есть официальные курсы, в том числе на русском языке.

PCWeek/UE: В этом году несколько вендоров анонсировали выпуск облачных DLP-систем. Насколько такие решения эффективны для защиты от утечек?

А.С.: Многие заказчики сейчас активно мигрируют в облако. Для них это значительная экономия денег на серверное оборудование, средства администрирования и поддержку. Однако облачная система закрывает только небольшую часть утечек, а ведь еще остаются рабочие станции, которые в любом случае необходимо защищать.

Преимущество облачных систем — легкость интеграции. Но не стоит забывать, что техническое внедрение DLP-системы — не самая сложная задача, поэтому значительной экономии от перехода в облако заказчик не получит в любом случае.

PCWeek/UE: Что предлагает Symantec в области DLP для мобильных устройств?

А.С.: В сфере защиты мобильных устройств не стоит ограничиваться только DLP-системами. На первое место встает процесс управления мобильными устройствами, контроль передачи информации между приложениями и т. д. Поэтому мы предлагаем комплексные решения, включающие и управление устройствами, и DLP-функционал.

PCWeek/UE: С какими сложностями сталкивается интегратор или заказчик в процессе внедрения? Сколько времени в среднем занимает проект по внедрению DLP-систем в компаниях?

А.С.: Самая большая сложность при внедрении в крупных организациях — отсутствие формализованных бизнес-процессов либо их описания. Иногда сложившихся бизнес-процессов нет вообще. Предпроектное обследование компании — первая фаза проекта — занимает больше всего времени. Необходимо понять, как перемещается конфиденциальная информация, кто может получить к ней доступ.

Поэтому время внедрения сильно варьируется в зависимости от готовности заказчика. Если формализованные процессы на предприятии прописаны, проект можно реализовать за несколько месяцев. Однако в крупных корпорациях много времени отнимают командировки в региональные офисы, согласование различных деталей и прочее. В результате проект комплексного внедрения (поддержка системы и ее полноценная настройка) может длиться год и дольше.

Что касается компаний с несложной инфраструктурой и небольшим количеством офисов, то техническая установка занимает лишь около месяца. Такой же период времени отводится для подписания договоров и составления технических заданий. Причем иногда данный этап занимает даже больше времени, чем само внедрение.

Самая большая сложность при внедрении в крупных организациях — отсутствие формализованных бизнес-процессов либо их описания

PCWeek/UE: Кто обычно занимается внедрением: ваш партнер или ИТ-департамент заказчика?

А.С.: Как правило, ИТ-департамент клиента не занимается внедрением DLP-системы. Максимум, к чему он привлекается, — настройка оборудования, интегрируемого с DLP. Обычно интегратор берет на себя ответственность за первоначальную настройку и обучает сотрудников компании.

PCWeek/UE: В каких случаях внедрения заканчиваются неудачей? Допустим, не удалось формализовать процессы или сопротивление сотрудников было так велико, что проект решили приостановить...

А.С.: Думаю, что можно говорить о небольшом проценте неудачных внедрений. Они происходят чаще всего вследствие ошибок партнеров, которые предложили неправильное решение. В результате либо заказчик не был готов к внедрению, либо оно ему в принципе не было нужно. Однако мы стараемся быть в курсе практически всех проектов по нашим DLP-решениям и контролируем партнеров, в том числе выясняем потребности заказчиков и помогаем в выборе.

PCWeek/UE: Кто является вашим основным конкурентом на рынке СНГ?

А.С.: Основные конкуренты — все западные производители, находящиеся в сегменте лидеров магического квадранта Gartner. Кроме того, на рынке работают и крупные российские производители DLP-систем.

НОВОСТИ

ПК

Ультрабуки остаются в тени ноутбуков

Впервые об ультрабуках как о новом виде компьютерных устройств Intel заявила в середине прошлого года на выставке Computex в Тайбэе. Под ультрабуками (этот термин стал торговой маркой производителя процессоров) Intel подразумевает устройства, внешне идентичные по форме ноутбукам, но гораздо тоньше их. Intel обязала производителей соблюдать некоторые условия при производстве ультрабуков — наличие SSD-накопителя, не менее 5 часов автономной работы, ускоренный запуск устройства и приложений на нем, толщина корпуса не больше 21 мм и др. Еще одним важным условием было соблюдение предельных цен на ультрабуки в пределах 1 тыс. долл. Но многие из этих условий производители ультрабуков проигнорировали, ссылаясь на то, что они не позволяют им удерживать рекомендуемую Intel цену. Согласно прогнозам Intel, по итогам текущего года ультрабуки будут занимать 40% сегмента ноутбуков. Но, как показывают данные исследовательской компании Barclays, прогнозы Intel пока что далеки от воплощения и на долю ультрабуков по итогам II квартала 2012 г. приходится лишь 5% от всех реализованных за этот период ноутбуков. Среди причин неудовлетворительных продаж этих устройств рыночные аналитики называют смещение пользовательских предпочтений в сторону планшетных устройств; ожидание выхода новой ОС Microsoft и множества гибридных планшетов на базе Windows 8, но главной причиной называется по-прежнему высокая стоимость ультрабуков.

При использовании материалов ссылка на сайт pcweek.ua обязательна

>>> НАЧАЛО НА С. 8
компаниях, где они используются для защиты корпоративных информационных ресурсов. Схожими по набору средств комплексами для крупного корпоративного сегмента являются системы для удаленного доступа мобильных сотрудников к ресурсам и сервисам корпоративной сети.

Rank	Categories Of Web Sites	Average Number Of Threats Found On Infected Web Sites	Major Threat Type Detected
1	Religion/ Ideologies	115	Fake Antivirus: 82%
2	Hosting/ Personal hosted sites	39	Trojans: 43%
3	Pornography	25	Trojans: 44%
4	Entertainment and Music	21	Fake Antivirus: 42%
5	Business/ Economy	17	Fake Antivirus: 62%
6	Technology/ Computer and Internet	17	Fake Antivirus: 54%
7	Travel	16	Fake Antivirus: 46%
8	Sports	13	Fake Antivirus: 69%
9	Automotive	11	Fake Antivirus: 41%
10	Shopping	9	Fake Antivirus: 63%

- Сайты со слабой защитой становятся легкой добычей для авторов вредоносного ПО
- Бизнес понимает, что клиенты не будут посещать зараженные сайты

Наиболее вредоносные сайты по категориям. Источник: Symantec, 2012

Василий Задворный: Сегодня действительно угрозы разделились: одни нацелены на информационные системы банка, другие — на клиентов онлайн-сервисов. Из наших продуктов и технологий для банков мы предлагаем услуги оценки защищенности информационных систем — тест на проникновение. В рамках этой услуги мы моделируем действия злоумышленников (как внешних хакеров, так и клиентов банка) с целью обнаружить существующие уязвимости и осуществляем попытку проникновения — взлома. Завершаются такие проекты разработкой рекомендаций, ведь для предприятий важно не только устранить существующие уязвимости, но и предотвратить их появление вновь. В части технологий защиты клиентов онлайн-сервисов мы продвигаем решение AOS (AhnLab Online Security), которое призвано защитить клиента, совершающего онлайн-транзакции, от всего спектра возможных угроз. Примечательно, что даже в случае, когда рабочая станция клиента заражена неким вредоносным ПО, решение AOS позволит совершить транзакцию, не допустив утечки критичных данных либо подмены реквизитов платежа.

Проекты по оценке защищенности — тест на проникновение — пользуются популярностью уже несколько лет. Если раньше основным заказчиком таких услуг были банки, то сегодня половина проектов происходит в компаниях из других отраслей. AOS вызывает интерес, однако в основном бизнес не готов тратить деньги на внедрение подобных систем, поскольку все риски на уровне договора перенесены на плечи клиента сервиса.

Владимир Удалов: Финансовые операции в Интернете стали неотъемлемой частью современной цифровой среды наряду с загрузкой медиафайлов и общением в социальных сетях. На сегодняшний день более 11% украинских семей обладают полным набором современных электронных устройств — ПК, ноутбук, смартфон, планшет. Но из-за повышенной активности мошенников пользователи переживают за сохранность данных.

Для защиты домашних пользователей «Лаборатория Касперского» предлагает обновленную версию Kaspersky Internet Security 2013. Угрозы сегодня постоянно видоизменяются, поэтому особое внимание в продукте уделено безопасности личных данных пользователей при совершении покупок в Интернете, а также любых банковских операций онлайн. Для этого в решение внедрена новая функция — «Безопасные платежи».

НАСКОЛЬКО БЕЗОПАСНО ОБЛАКО?

Исследования аналитиков показывают, что многие компании считают защиту облаков надежной. Но так ли это на самом деле? Аналитики в области ИБ с этим категорически не согласны. Чтобы расставить точки над «i», мы предложили экспертам ответить на следующие вопросы:

Какие условия необходимо выполнить, чтобы облака были безопасны? Какие технологии вы предлагаете для защиты всех хранящихся в облаке данных?

Геннадий Карпов: На мой взгляд, широко обсуждаемая тема облачной безопасности все еще имеет ярко выраженную эмоциональную окраску. Это вполне естественно, поскольку процесс привыкания к новой парадигме производства и потребления ИТ-сервисов пока далек от завершения — сменить технологии все-таки оказалось проще, чем обеспечить их восприятие людьми. Если же сместить точку зрения от эмоциональной к рациональной, то становится очевидным, что мы имеем дело с классической задачей, которая должна быть решена в новом окружении и с использованием новых технологий. Как ни удивительно это может прозвучать, во многих случаях новая среда позволяет решать задачи безопасности во всех ее проявлениях более просто и надежно, чем в унаследованных корпоративных информационных системах.

Не все облака одинаково полезны. И публичное облако, скорее всего, не сможет дать эффективный ответ на актуальную для корпоративного заказчика модель угроз. Во многом это определяется его природой — максимально облегченный доступ через Интернет для широкой и заранее неопределенной аудитории пользователей. Но существуют и другие типы облаков коллективного использования, которые значительно лучше приспособлены к потребностям корпоративного сегмента рынка.

Например, гипероблако De Novo построено по модели Trusted Cloud. Она предполагает доступ к гипероблаку ограниченного количества надежно идентифицированных пользователей, изоляцию выделенных им виртуальных датацентров, приоритетное использование персональных каналов «точка-точка» и жестко контролируемое взаимодействие с Всемирной сетью. В операционной модели Trusted Cloud используются практически те же технические и организационные инструменты безопасности, что и в зрелых корпоративных инфраструктурах. Среди них: IDS/IPS, блокирование вредоносного контента, средства защиты от аппаратных отказов и логического разрушения данных, разделение ролевых функций персонала и работающая политика информационной безопасности, доведенная до уровня технологических карт.

Мирослав Мищенко: Провайдер облака должен гарантировать его безопасность, для чего необходимо обеспечить как защиту сети, так и физической среды. Поэтому важно выбрать провайдера с хорошей репутацией, опытом и качественными решениями в области сетевой безопасности и операционных сред. Кроме того, он должен продемонстрировать, что все риски в области ИБ были проанализированы и считаются приемлемыми, что система защиты протестирована, и он способен управлять угрозами. Необходимо проверить, как провайдер облака реагирует на инциденты, например, есть ли у него центр по обеспечению безопасности (ЦОБ).

Также важно оценить, какие физические меры безопасности предприняты в отношении того помещения, где хранятся данные. Установлена ли система контроля доступа, есть ли видеонаблюдение? Рекомендуется выбирать провайдера облака, который гарантирует меры физической безопасности в соответствии с SAS 70 или ISO 9000.

В облачных вычислениях несколько пользователей используют одно и то же приложение или аппаратное обеспечение. Это предполагает, что информация нескольких организаций находится на одной физической системе. Поэтому крайне важно убедиться, что система сегментирована правильно, данные и приложения полностью отделены друг от друга. Тем не менее, виртуальные среды работают иначе, чем традиционные серверы. Последние контролируют весь трафик через физический коммутатор Ethernet или маршрутизатор. В виртуальной среде поток данных проходит через виртуальный адаптер. Это создает так называемое «белое пятно» в соединении между центром обработки данных и конечными пользователями, и в итоге — потенциальную угрозу для безопасности. Настройка физического или виртуального устройства защиты между поставщиком облака и заказчиком окажется разумным решением, так как поможет обеспечить правильное сочетание производительности и контроля в пределах потоков данных.

Олег Просветов: Основная формула, которой должны пользоваться компании, переводящие всю инфраструктуру в облака, выглядит следующим образом: «Успех = систематический подход + оценка рисков + четко прописанные политики».

К переходу в облака нужно подходить систематически, не стоит переносить туда сразу всю инфраструктуру. Переход должен быть постепенным, осознанным, вначале нужно понять, насколько облака помогут сэкономить на ресурсах, капиталовложениях и т.п.

Компаниям стоит проанализировать все плюсы и минусы таких преобразований. Перевод инфраструктуры во внешние облака чем-то похож на аутсорсинг — работу со сторонней организацией, когда все полномочия четко разграничены и прописаны в договоре.

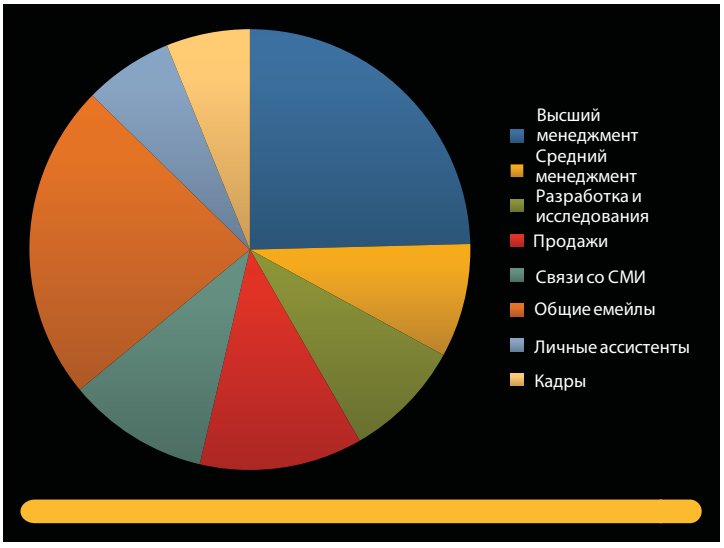
Кроме того, при переводе ИТ-инфраструктур в облака у компаний должна быть четкая стратегия, ведь это привнесёт новые риски и угрозы. Вот почему понадобятся дополнительные защитные и организационные меры: шифрование, отказоустойчивость сети, процессы взаимодействия с техподдержкой и т.д.

Среди наиболее актуальных и востребованных заказчиком облачных технологий можно назвать хранение резервных копий в облаке, архивирование почты и т. д. Так, Symantec предлагает услугу облачного резервного копирования. Она позволяет небольшой организации получить полноценную систему резервного копирования. Мы предлагаем бэкап в виде услуги, так как зачастую компаниям не хватает ресурсов для организации собственной инфраструктуры, а общедоступные облака не вызывают доверия. В свою очередь Symantec предоставляет многоуровневую систему отказоустойчивости корпоративного класса для небольших компаний.

Новая облачная платформа Symantec O3 дает возможность контролировать использование облачных ресурсов, предлагая единую точку входа корпоративных пользователей к внутренним и внешним облачным ресурсам из любой точки мира и с любого устройства. В конце осени выйдет дополнение к платформе, которое позволит контролировать передачу данных (загрузки и скачивания, отправка файлов и т.д.) и интегрировать облачные системы с системами шифрования и контроля за утечками данных (DLP).

Илья Магась: Поручать третьей стороне обрабатывать ваши данные можно в двух случаях: либо если они

ПРОДОЛЖЕНИЕ НА С.15>>>



Целевые атаки на сотрудников различных департаментов. Источник: Symantec, 2012

При использовании материалов ссылка на сайт pcweek.ua обязательна

СРЕДСТВО КОНТРОЛЯ ДЛЯ ВЫСШЕЙ КАСТЫ

ОЛЕГ ПИЛИПЕНКО

ИНТЕРВЬЮ

Любая организация, которая заботится о своей безопасности, старается ограничить права пользователей, уменьшив тем самым возможности для утечки данных или злонамеренного причинения вреда системе. Однако в ИТ-структуре предприятия есть особая «каста неприкасаемых» — системные администраторы, обладающие максимальными правами доступа, действия которых сложно контролировать. Не так давно компания Quest Software выпустила специальные решения, позволяющие осуществлять тщательный мониторинг деятельностью даже тех ИТ-специалистов, которым предоставлены максимальные права доступа. О преимуществах и специфике данных решений рассказывает Евгений Гончаренко, менеджер по развитию бизнеса Quest в группе компаний «БАКОТЕК».

PCWeek/UE: Евгений, что собой представляет Quest One Privileged Account Management? Какие преимущества получает заказчик при покупке этих решений?

ЕВГЕНИЙ ГОНЧАРЕНКО: Решение для управления доступом Quest One Privileged Access Management от компании Quest Software — это проверенный временем комплект интегрированных модульных технологий. Он разработан специально для удовлетворения растущих требований к безопасности и соответствию стандартам, связанных с управлением привилегированной идентификацией и контролем привилегированного доступа.

В подобных решениях заинтересован менеджмент компаний, который испытывает необходимость контролировать ИТ-специалистов с привилегированным доступом (чаще всего речь идет о системных администраторах). Проблема в том, что обычно создают только одну учетную запись с максимальными правами доступа (например, root в ОС Linux), но ее используют несколько администраторов. Если служба безопасности компании зафиксировала в системе какие-либо несанкционированные действия, то понять, кто и когда их произвел, достаточно сложно. Именно в таких случаях поможет продукт Quest One Privileged Password Manager, который позволяет с помощью так называемой «тикетной» системы (системы заявок) отправить запрос на выдачу пароля. В зависимости от настроенной политики пароль выдается автоматически либо после подтверждения офицером, отвечающим за безопасность в компании. Но даже в случае позитивного ответа системы администратор может использовать пароль только в течение определенного времени. По истечении этого времени, система меняет пароль, и старый уже не будет действовать. Таким образом, решение Privileged Password Manager гарантирует, что при необходимости обеспечить администраторам доступ с повышенными правами он будет предоставлен согласно установленной политике с выдачей соответствующих разрешений. При этом все действия администраторов можно будет контролировать, а пароль будет изменен сразу же после завершения работы использовавшим его сотрудником.

В свою очередь, с помощью Quest One Privileged Session Manager можно осуществлять мониторинг всех действий в системе, где работает ИТ-администратор. Решение обеспечивает единую точку контроля, с которой менеджер безопасности способен авторизировать соединения, ограничивать доступ к специфическим ресурсам, просматривать активные соединения. Фактически это является неким аналогом видеозаписи всех действий ИТ-специалиста во время работы, например, на серверной системе Linux, Windows, Exchange Server и т. д. При этом продукт генерирует предупреждение, если продолжительность сессии превышает заранее установленный временной лимит.

С точки зрения архитектуры решение Quest One Privileged Access Management — это единое устройство, в котором активируется тот или иной продукт в зависимости от купленных лицензий. Его важной особенностью является то, что функционал по разделу полномочий разнесен на аппаратном уровне. Кроме того, поскольку это физическое устройство, исключается возможность взлома со стороны администратора. Ведь если используется виртуальная машина и виртуальное устройство, то администратор может «потушить» эту машину и таким образом снять защиту. А в случае данного решения сервер можно остановить разве что физически, но ведь доступ в серверное помещение получить не так-то легко.

Программно-аппаратный комплекс Quest One Privileged Access Management

Продукт Quest достаточно прост с точки зрения введения в эксплуатацию. Он обладает интуитивно-понятным интерфейсом, хорошо интегрируется с другими системами, в том числе с Active Directory, SIEM-системами и прочими. Кроме того, вся информация, которую хранит устройство, защищена на уровне аппаратного шифрования, что гарантирует защиту от вторжений и взломов.

PCWeek/UE: Продукт интегрирован с другими решениями Quest или его можно использовать автономно?

Е.Г.: Компания Quest всегда заявляла, что не производит дорогостоящих решений, якобы покрывающих все проблемы предприятия. Вместо этого компания создает мозаику, в которую можно интегрировать разные инструменты, предназначенные для решения различных задач. В результате заказчик может выбрать именно тот комплект решений, который оптимально ему подходит. При создании данного семейства продуктов вендор придерживался такой же философии. Эти решения могут быть вполне самодостаточными и работать отдельно, в то же время они бесшовно интегрируются с системами мультифакторной идентификации Quest Defender, системой управления пользователями Quest One Identity Manager, системой сбора логов Quest InTrust и т. д.

Стоит отметить, что программно-аппаратный комплекс Quest One Privileged Access Management построен на базе серверов Dell. Не секрет, что Quest и Dell давно связывают партнерские отношения, и после слияния этих компаний интеграция их решений усилится еще более.

PCWeek/UE: Каков диапазон стоимости данных продуктов?

Е.Г.: Продукты достаточно гибко лицензируются, их цена варьируется в зависимости от размера организации или ее требований. Но в среднем их стоимость лежит в той же ценовой категории, что и у «коллег по цеху».

Евгений Гончаренко

PCWeek/UE: Сколько времени занимает внедрение продукта?

Е.Г.: Весь процесс инсталляции от включения в розетку до начала использования занимает максимум один день. Ведь в отличие от многих конкурентных продуктов, Quest поставляет свою разработку в виде программно-аппаратного комплекса, представляющего собой готовое решение «под ключ». Заказчику остается только включить его в сеть, произвести базовое конфигурирование и подключить необходимые системы.

PCWeek/UE: Кого вы видите заказчиками таких решений? Крупный корпоративный сектор или СМБ-сегмент?

Е.Г.: Одной из причин покупки такого продукта является требование соответствовать стандартам. Ведь это решение помогает выполнить определенные требования по СУИБ ISO 27001, PCI DSS и т. д. Таким образом, главными потребителями являются финансовые учреждения. Кроме того, как Privileged Session Manager, так и Privileged Session Manager оптимальны для компаний с повышенными требованиями к внутренней безопасности.

Отмечу также, что подобные инструменты могут быть полезны организациям, прибегающим к ИТ-аутсорсингу, когда часть работы по управлению и администрированию выполняют третьи компании. Поэтому сотрудники службы безопасности хотят иметь инструмент, позволяющий следить за работой специалистов, которые подключаются к корпоративным системам в процессе их обслуживания. Privileged Session Manager дает возможность через веб-портал запрашивать доступ к определенному устройству, серверу или базе данных. После подтверждения пароля ИТ-специалист прямо в веб-портале видит рабочий стол сервера и выполняет все необходимые административные функции. В то же время он заполняет запись с так называемым тегированием для облегченного поиска в дальнейшем.

В целом география заказчиков очень широкая. Мы продвигаем продукты Quest не только в Украине, но и в Латвии, Литве, других странах. Там заметный интерес к этим технологиям проявляют правительственные организации и силовые структуры. В перспективе мы планируем заинтересовать и украинские государственные учреждения, которые испытывают потребность в ограничении доступа к каким-либо системам либо в гранулярном контроле. Но вначале мы хотим «прощупать» рынок. К примеру, наблюдаем интерес к решению среди управляющих подразделений холдинговых компаний, где хранится самая важная информация о различных корпорациях, входящих в группу. Активно интересуются нашими продуктами и финансовые организации.

PCWeek/UE: Как давно начались поставки этих решений в Украину?

Е.Г.: С конца прошлого года решения стали доступны в нашем партнерском канале. А с начала 2012-го мы начали активно развивать это направление. У нас уже есть сертифицированные специалисты по продуктам, которые могут помочь партнерам и клиентам провести тестирование. Кроме того, в лаборатории «Бакотек» имеется тестовое оборудование, на котором проводятся демонстрации.

НОВОСТИ

ПРОЕКТЫ

Внедрение программно-аппаратного комплекса Oracle в ДК «Укртрансгаз»

В ДК «Укртрансгаз», крупном поставщике газа в Украине, завершено развертывание мощного программно-аппаратного комплекса Oracle, который стал частью корпоративной стратегии по централизации ИТ-инфраструктуры и оптимизации бизнес-процессов. Новое решение представляет собой аппаратную платформу для работы ERP-системы на СУБД Oracle и призвано обеспечить высокую вычислительную мощность, надежность и отказоустойчивость.

Дочерняя компания «Укртрансгаз» является главным транзитером российского природного газа в Европу. Основными задачами предприятия являются обеспечение бесперебойной транспортировки природного газа, эффективного функционирования и развития газового комплекса, более полного удовлетворения потребностей промышленных и бытовых потребителей сырьем и топливно-энергетическими ресурсами.

В рамках динамичного развития компании было принято решение оптимизировать бизнес-процессы и централизовать работу 17 структурных подразделений ДК «Укртрансгаз». Развертывание ERP-системы, которая охватила более пяти тысяч сотрудников, потребовало использования нового эффективного оборудования, оптимизированного для выполнения системы управления базами данных Oracle и обладающего наилучшим соотношением цена/производительность.

В качестве стратегической консолидационной платформы для уровня баз данных и серверов приложений был выбран сервер Sun SPARC Enterprise M9000-64 класса high-end, обеспечивший выполнение критически важных задач ДК «Укртрансгаз» в режиме 24x7x365. Новая инфраструктура предприятия также включает универсальные высокопроизводительные серверы Oracle SPARC T4-4 для уровня серверов приложений под управлением ОС Solaris. Системы хранения данных Pillar Axiom 600 обеспечивают лучший в отрасли уровень использования емкости СХД без потерь в производительности, что было критически важным для этого проекта. Для архивного хранения информации была выбрана модульная библиотека STORAGETEK SL500.

«Программно-аппаратный комплекс Oracle с использованием архитектуры SPARC и платформы Pillar Axiom сегодня полностью поддерживает бизнес-задачи компании и является фундаментом для дальнейшего развития. Скорость и надежность были нашими ключевыми требованиями, поэтому СУБД Oracle для ERP-проекта определила подходы к архитектуре и выбору аппаратной платформы, что в результате позволило минимизировать риски и добиться высочайшей производительности всего решения от одного вендора», — отмечает директор филиала «Укргазтехсвязь» ДК «Укртрансгаз» Виталий Волосецкий.

При использовании материалов ссылка на сайт pcweek.ua обязательна

ИНТЕРВЬЮ

БІЛЬШІСТЬ ЛЮДЕЙ ДУМАЄ ЛИШЕ ПРО ЗРУЧНІСТЬ, А НЕ ПРО БЕЗПЕКУ

ОЛЕГ ПИЛИПЕНКО

Сьогодні питання інформаційної безпеки порушують не лише фінансові організації, а й промислово-індустріальний сектор. При цьому компанії зацікавлені не тільки в зовнішньому захисті, а й обороні від інсайдеру. Про ці та інші тенденції на ринку інформаційної безпеки України розповідає Василь Задворний, керівник відділу IT-консалтингу компанії Інком.

PCWeek/UE: Василю, які тренди останніх років ви можете відзначити на ринку інформаційної безпеки України. Що змінилося порівняно з кризовим періодом?

ВАСИЛЬ ЗАДВОРНИЙ: Можна виділити кілька основних тенденцій. Так, раніше компанії при забезпеченні інформаційної безпеки в 95% випадків розв'язували всі проблеми за допомогою простих і загальнодоступних рішень: антивірусного програмного забезпечення, мережевих екранів тощо. Сьогодні все змінилося, і найперший тренд, який можна визначити, — це бажання клієнтів використовувати складні продукти. Велику частку наших проектів зараз займають складні рішення, пов'язані не лише з упровадженням певної системи, а й побудовою роботи персоналу та процесів управління.

Василь Задворний

Причина в тому, що ринок наситився простими рішеннями і хоче рухатися далі. З'являються складніші загрози, на які треба реагувати відповідно і вчасно. А саме в цьому здатні допомогти SIEM-рішення (Security Information and Event Management — система керування інформацією про події та стан безпеки), які вже півтора-два роки популярні на ринку України. Вони дозволяють виконувати моніторинг подій інформаційної безпеки та автоматично знаходити підозрілі ситуації, на які людина просто не звернула б увагу. Класичний приклад: користувач увів пароль у свій комп'ютер та увійшов у систему, але попередньо не відмітився карткою на прохідній і не пройшов СКД (систему контролю фізичного доступу). SIEM-рішення здатне виявити такі деталі та повідомити центр інформаційної безпеки.

Збільшується попит і на системи класу DLP-захисту від витоку інформації. Зростає інтерес до рішень захисту систем керування базами даних (DAM) та управління обліковими записами (IdM). Загальний тренд стосовно продуктів — постійно з'являються нові й більш складні рішення. Вони вимагають впровадження не лише технічної частини, а й процесної. Очевидно, що їх появу зумовлює збільшення кількості загроз та інцидентів.

Другою тенденцією є зміна профілю клієнтів. Якщо донедавна інформаційна безпека була прерогативою фінансових організацій, то вже близько півтора року ми спостерігаємо знакові проекти в промислово-індустріальному секторі економіки. Багато компаній, не пов'язаних напряму з фінансами, вимагають для себе високого рівня інформаційної безпеки. Ми думаємо, це відбувається з тієї причини, що фінансова криза загострила конкурентну ситуацію на ринку, відповідно зросла й недоброякісна конкуренція. У деяких наших клієнтів звільнені під час кризи працівники намагалися таким чином помститися колишнім роботодавцям.

Третій тренд — збільшення законодавчих вимог до гравців ринку. Це законодавчі або галузеві ініціативи, спрямовані на учасників ринку. Зокрема, постанова НБУ про стандарт забезпечення безпеки банків СОУ Н НБУ 65.1 СУІБ 1.0:2010, впроваджений на всій території України, є серйозною рушійною силою. Загострилися вимоги міжнародних організацій до впровадження їхніх стандартів. Свою роль зіграв і Закон України «Про захист персональних даних».

І нарешті, четвертий тренд — підвищення рівня інформаційної безпеки в компаніях загалом. Почастішали атаки, спрямовані не тільки на іміджеві марки, а й на зниження доступності сервісів. DDoS-атаки (розподілені атаки) можуть починатися з комп'ютерів, розташованих у будь-якій частині світу, і зупинити роботу банківського сайту чи певних сервісів компанії. Відповідно компанії втрачатимуть гроші, хоча власне організація такої атаки коштує відносно небагато.

PCWeek/UE: Нині ринок інструментів для захисту баз даних розширився. Що є більш популярним: засоби інформаційної безпеки, вмонтовані в СУБД, чи якісь зовнішні інструменти?

В.З.: Інструментів стало більше саме тому, що можливостей засобів, вбудованих у СУБД, недостатньо. Так, використання функціоналу СУБД дає можливість покрити деяку кількість базових загроз, а там уже кожен для себе вибирає, які загрози для нього важливіші й чи потрібні допоміжні засоби. Вбудовані засоби захищають СУБД, наприклад, від підбору паролів. А зовнішні інструменти вирішують більш складні завдання: захищають від неавторизованого доступу до даних адміністраторами, неавторизованої зміни даних легітимними користувачами тощо.

PCWeek/UE: Використання мобільних пристроїв на роботі становить реальну загрозу для інформаційної безпеки?

В.З.: Мобільні пристрої — це велика проблема. Жартома кажучи, Стів Джобс зробив усім «ведмежу послугу», так розкрутивши свій iPad, що ним тепер користуються майже всі топ-менеджери. І найчастіше пристрої налаштовують з прямим доступом до корпоративної пошти через Інтернет. А планшет зі збереженою на ньому інформацією можна просто загубити, тож не завжди навіть встановлення захисного програмного забезпечення є виходом із ситуації. Та й не для всіх моделей і операційних систем є відповідне ПО. Треба глибше розглядати питання інформаційної безпеки: класифікації інформації, обмеження доступу до контенту на рівні його генерації тощо.

PCWeek/UE: Розкажіть про найцікавіші проекти в області інформаційної безпеки, які вам доводиться реалізовувати.

В.З.: Частина нашої практики — виконання тестів на проникнення. Це цікаві проекти з багатьма невідомими, де неможливо передбачити, який буде результат. Тест на проникнення — особливий вид активного аудиту, імітація хакерської атаки, стрес-тест на визначення здатності компанії протистояти реальним атакам ззовні або зсередини. Ми є одними з лідерів цього напряму в Україні. У нас у штаті працює сертифікований етичний хакер (Certified Ethical Hacker — міжнародна сертифікація для спеціалістів з таких робіт). Маємо потужну команду: наші спеціалісти навіть увійшли в десятку кращих на змаганнях хакерів, які відбулися нещодавно в Росії.

Якщо раніше всіх цікавив лише зовнішній захист, останнім часом збільшилося замовлення тестів на внутрішнє проникнення. Керівників цікавить, яку загрозу може становити для компаній навіть діяльність пересічного бухгалтера. Проведені нами тести, як правило, показують, що компанії зсередини слабо захищені: 80-90% проектів з тестів на внутрішнє проникнення закінчувалися отриманням повного доступу до корпоративних баз даних. А там лишається лише крок до керування всіма транзакціями в фінансових системах.

Із зовнішніми тестами ситуація набагато краща. Ззовні лише інколи вдається отримати доступ до керування IT-інфраструктурою. У 20-40% проектів знайдена інформація не дозволяла говорити про велику загрозу для компанії.

PCWeek/UE: Як запобігти проникненням у корпоративні системи? Які є для цього засоби?

В.З.: Найслабшим місцем лишається парольна політика. Сучасна техніка дозволяє підбирати мільйони паролів за секунду, навіть мільярди, якщо використовувати потужність відеокарт. Зазвичай, ми легко розкриваємо паролі в 75-80% наших проектів. Якщо ми вже отримали доступ до бази хешів паролів користувачів (а її нескладно знайти), то паролі будуть підібрані. І це в умовах обмеженого часу при виконанні тестів на проникнення. А якщо часу більше? Ось, наприклад, після злому соціальної мережі LinkedIn було опубліковано 6,5 млн хешів паролів облікових записів користувачів. Зазвичай, на таких прикладах наша команда тренує свої навички та відпрацьовує методики. В ситуації із LinkedIn вдалося підібрати більше 75% паролів, що містили від 6 до 20 символів різної складності, а деяка їх частина навіть відповідала рекомендованим правилам складності паролів. Для того, щоб підбирати паролі, взагалі достатньо потужного домашнього комп'ютера. І зловмисникам навіть не треба створювати для цього складні програми.

Середній пароль у споживачів рідко коли перевищує 6-8 символів, і вони підбираються дуже швидко. Навіть якщо довжина паролю перевищує 15 символів, підібрати його не завжди буде важко. Для цього використовують власні методики, на базі яких генеруються потенційні паролі користувачів. Виходячи навіть з назви компанії та її найбільш популярного продукту, можна припустити, що в когось із користувачів напевно буде такий пароль. Реальна парольна політика та періодичний аудит використання паролів відіграє велику роль для захисту інформації.

Важливий аспект інформаційної безпеки — робота з користувачами. Жодна технологія не буде працювати, якщо люди нею не користуються. Можна впроваджувати найсильніші системи захисту, найкращу парольну політику, але коли немає роз'яснення, для чого це потрібно, працівники просто записуватимуть паролі на папірці та вішатимуть їх на монітор, або вибиратимуть паролі, які комфортно запам'ятовувати через розташування символів на клавіатурі, наприклад, «1qaz@WSX»!

Так, при виконанні одного з тестів на проникнення, в якому було отримано адміністративний доступ до мережевої інфраструктури, системний адміністратор лише через місяць проглянув журнал системи моніторингу і побачив, що вона йому сигналізувала. Отже, організаційні заходи бувають набагато дешевшими й ефективнішими засобами інформаційної безпеки. Ось вам приклад: у найбільших консалтингових компаніях світу ноутбуки, які залишають в офісі і потенційно можуть вкрасти, обов'язково пристібають до якогось стаціонарного предмета. Якщо працівник не виконує цієї умови, його штрафують.

PCWeek/UE: Хто найчастіше є замовником тестів на проникнення? Фінансові організації, телекомоператори?

В.З.: Фінансові організації стабільно цікавляться цими послугами, але становлять тільки 50% наших клієнтів. Інша половина — промисловість, енергетика, роздрібний сектор, телеком-оператори.

Тести на проникнення популярні тому, що IT-відділу легше показати менеджменту реальний звіт про цілком можливі «аварійні» ситуації, аніж розповідати про класифікацію даних чи про вартість якогось «заліза». Однак інтерес клієнтів став більш сфокусованим. Їм цікаві не просто звіти, а кількість виявлених вразливостей, підтримка при їх усуненні, перелік проектів, які можна було б утілити.

PCWeek/UE: Як довго триває власне тест на проникнення?

В.З.: Буває, що дірки в захисті настільки великі, що проникнення відбувається протягом лічених днів. Але в основному для того, щоб результати були репрезентативними, треба попрацювати принаймні місяць. Чим більше часу — тим більше результатів, бо багато тестів пов'язано з очікуванням певних подій у системі клієнта: хтось переслав інформацію, вдалося підібрати паролі та інше.

Під час тестів на проникнення ми використовуємо два варіанти поведінки. Якщо багато знаємо про інфраструктуру клієнта, тест називається whitebox, коли не маємо такої інформації — blackbox. Так само спеціалісти IT/ІБ-підрозділів клієнта можуть знати про нашу роботу (це буде whitehat) або не знати (blackhat). Вибір моделі залежить від того, що саме ми хочемо перевірити. Якщо клієнт знає про проникнення, він може не втручатися в наші дії, а ми перевірятимемо лише технічну складову. Коли ж він не поінформований про наші дії (крім осіб, які підписували контракт), тоді тестуємо не лише технічну складову, а й організаційну. Тобто виявляємо, наскільки швидко працівники відреагують і виявлять проникнення.

PCWeek/UE: Скільки осіб працює над проектом? Що пропонує клієнтам ваша компанія після його завершення?

В.З.: Працює від 3 до 7 осіб, залежно від проекту. Наприкінці ми розробляємо рекомендації і зазвичай надаємо консалтингову підтримку при їх виконанні. Усунення першочергових зауважень займає 3-4 місяці і не потребує великих фінансових витрат. Після цього періоду ми, як правило, перевіряємо усунення можливих загроз.

PCWeek/UE: Чи практикується в компаніях ваших клієнтів двофакторна аутентифікація: мишка з біосканером, аутентифікація за відбитками пальців...

В.З.: Двофакторну аутентифікацію вимагають багато стандартів, наприклад PCI DSS. Вона дає вагомі переваги, навіть якщо не використовувати біометричну інформацію, а лише маркер доступу з певними цифрами та пароль, який ви знаєте. Але системи біометрії коштують досить дорого для масового впровадження. Частіше українські компанії використовують апаратні токени в якості другого фактору аутентифікації та лише для найбільш критичних інформаційних систем.

Багато західних компаній користується навіть більш простою схемою. Вони видають робітникам папірець з тимчасовими паролями й ті використовують паролі по черзі: один, другий, третій. Це і є додатковий фактор аутентифікації — використання згенерованої інформації. Але впровадження таких систем робить сам процес аутентифікації важчим для користувача. А у випадку інформаційних технологій більшість людей думає про зручність, ніж про безпеку. Тому такі засоби можуть просто викликати нерозуміння користувачів.

При использовании материалов ссылка на сайт pcweek.ua обязательна

IPV6 И СЕТЕВАЯ БЕЗОПАСНОСТЬ

РОБЕРТ ХИНДЕН

В начале июня состоялся всемирный запуск интернет-протокола IPv6. Основные интернет- и контент-провайдеры уже начали использовать этот протокол на постоянной основе, что вызвало резкий скачок трафика как собственно IPv6, так и туннельных протоколов — 6in4, Teredo и др. Учитывая все более активное применение IPv6, официальный его запуск стал значительным шагом вперед. День «сдачи IPv6 в эксплуатацию» прошел, но ответить на вопросы относительно безопасности нового протокола специалистам еще предстоит.

ПРОЕКТЫ

Серьезной проблемой является способность неавторизованных туннельных протоколов скрывать трафик IPv6, что позволяет обходить устройства сетевой защиты. Чтобы перекрыть эти обходные пути, специалисты должны четко представлять принцип работы переходных механизмов IPv6.

Легко понять, для чего организациям необходим переход на IPv6. Запас нераспределенных адресов IPv4 уже практически исчерпан. Каждое устройство, подключенное к Интернету, идентифицируется по IP-адресу; в протоколе IPv4-адрес имеет длину 32 бита, то есть всего уникальных IP-адресов — 232. IPv6 расширяет это количество до 2128. Протокол IPv4 до недавних пор справлялся со своей задачей, однако из-за того, что к Интернету подключается все больше и больше устройств, дни его, можно сказать, сочтены. У IPv6 есть и другие преимущества перед IPv4, например упрощенное выделение адресов.

Переход на IPv6 ставит перед организациями, в которых развернуты компьютерные сети, ряд важных задач

Переход на IPv6 ставит перед организациями, в которых развернуты компьютерные сети, ряд важных задач. Им следует уделять вопросам безопасности протокола IPv6 такое же серьезное внимание, как и IPv4. Ответственным за практическую реализацию систем безопасности необходимо знать основы нового протокола, чтобы правильно организовать переход. В Интернете уже опубликованы советы и рекомендации по этому поводу, в том числе разработанные Национальным институтом стандартов и технологий (NIST, США).

Если устройства сетевой защиты поддерживают IPv6, сейчас самое время включить их. В некоторых операционных системах, например Windows Vista и Windows 7, механизмы перехода на IPv6 активны по умолчанию. Это означает, что возможности нового протокола задействуются без ведома ИТ-специалистов, и трафик начнет следовать в обход межсетевых экранов и систем предотвращения вторжений.

Хосты и маршрутизаторы, использующие IPv6, соединяются с другими IPv6-устройствами в сетях IPv4 посредством туннелей. Проблема заключается в том, что туннели способны пробивать межсетевые экраны. А значит, злоумышленники могут обмануть систему безопасности и получить доступ к ресурсам локальной сети извне. Следует тщательнее просчитывать и по возможности минимизировать использование туннельных протоколов (6to4 и т.п.) для поддержки перехода на IPv6.

Сетевым администраторам необходимо иметь в виду, что протокол IPv6 уже может работать в корпоративной сети и служить скрытым каналом для ботнетов и хакеров. Даже если трафик IPv6 в организации невелик, инфраструктура безопасности должна уметь его обнаруживать и обрабатывать. Ведь всем ясно, что невидимку поймать невозможно.

Что касается безопасного развертывания IPv6, ключевыми словами здесь являются «обнаружение» и «контроль». Системы сетевой защиты в организациях должны поддерживать IPv6 и корректно обрабатывать его трафик. Иногда это потребует обновления систем, поскольку системы предотвращения вторжений и межсетевые экраны прежних поколений могут не контролировать трафик IPv6. К счастью, в течение последних нескольких лет большинство ведущих производителей систем сетевой защиты обеспечили в них поддержку IPv6. Организациям следует проконсультироваться с поставщиками по вопросу всей необходимой функциональности в системах и начать внедрение нового протокола в своих сетях. Помочь здесь способны официально утвержденные программы тестирования IPv6, например программа сертификации USGv6, разработанная специалистами NIST.

По мере роста числа организаций, внедряющих IPv6, администраторам необходимо следить за работой механизмов перехода и конфигурациями устройств, не допуская несанкционированного открытия доступа в сеть извне.

Мониторинг всего сетевого трафика — важное условие для сетевой безопасности

Мониторинг всего сетевого трафика — важное условие для сетевой безопасности. Все обнаруженные неавторизованные туннели должны своевременно блокироваться, чтобы защитить сеть от атак. Внедрение IPv6 в глобальном масштабе неизбежно. Поэтому сегодня нужно предпринять все меры для того, чтобы переход на новый протокол не подверг корпоративные сети дополнительным угрозам вторжений.

Автор — сотрудник Check Point Software Technologies Ltd. и один из разработчиков IPv6. В 2008 г. он стал одним из лауреатов премии IEEE Internet Award за свои передовые разработки в области интернет-маршрутизаторов.

БИЗНЕС РИСКУЕТ, ПЕРЕВОДЯ КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ В ОБЛАЧНЫЕ СИСТЕМЫ ХРАНЕНИЯ

НАТАН ЭДДИ

Согласно глобальному опросу более 4 тыс. менеджеров и ИТ-руководителей, проведенному исследовательской организацией Ponemon Institute по заказу корпорации Thales, более 80% компаний уже перенесли или планируют перенести конфиденциальные данные в облачные платформы хранения информации. Однако, как говорит исследование, получившее название «Шифрование в облаке» (Encryption in the Cloud), компании могут узнать, каким образом защитить критически важные данные и чьей ответственностью это является.

Свыше половины опрошенных сообщили, что их организации в настоящее время переносят чувствительную или конфиденциальную информацию в облако. Из них 64% считают, что именно провайдер облачных сервисов несет основную ответственность за защиту этой информации. В то же время около двух третей респондентов не знают, что провайдеры таких услуг действительно делают для защиты доверенных им конфиденциальных сведений.

36% участников опроса сообщают, что их организация несет основную ответственность за управление ключами шифрования, а 22% уверенны, что именно провайдер облачных услуг отвечает за управление такими ключами. Результаты исследования показывают, что даже в тех случаях, когда шифрование производится внутри корпоративной сети, более половины респондентов передают управление ключами облачному провайдеру.

«Это довольно серьезно, когда около половины участников опроса признают, что их компании уже передают свои конфиденциальные данные в облако, и при этом 39% из них считают, что в результате ситуация с информационной безопасностью ухудшилась, — подчеркнул в своем сообщении Ларри Понемон (Larry Ponemon), председатель правления и основатель Ponemon Institute. — Это ясно показывает, что для большинства компаний экономические преимущества от применения облачных технологий перевешивают риски в области безопасности… Однако особенно интересно отметить, что те самые организации, у которых был очень высокий общий уровень информационной безопасности, оказались в первых рядах сторонников передачи информации этого класса в облако. Возможно потому, что они лучше других понимают, как и где применять такие инструменты, как шифрование, для защиты своих данных и сохранения контроля над ними».

Отчет показывает разделение респондентов практически поровну на тех, чья организация применяет устойчивое шифрование данных до отправки их

Сохранение контроля над чувствительной и конфиденциальной информацией является сегодня задачей первостепенной важности для большинства компаний

облачному провайдеру, и на тех, кто полагается на шифрование данных провайдером. Треть опрошенных сообщила, что их организации весьма вероятно приступят к переносу конфиденциальных данных на облачные ресурсы в ближайшие два года. Это предполагает возрастание риска нарушения конфиденциальности просто в силу увеличения объемов данных, размещаемых различными компаниями на облачных системах хранения.

«Сохранение контроля над чувствительной и конфиденциальной информацией является сегодня задачей первостепенной важности для подавляющего большинства компаний. Для любой организации, все еще взвешивающей преимущества облачных вычислений и сопутствующие им угрозы в области безопасности, важно понимать, что шифрование представляет собой один из наиболее важных инструментов защиты данных, — отметил Ричард Мулдс (Richard Moulds), вице-президент по стратегии отделения Thales e-Security. — Однако любой тип шифрования имеет смысл только тогда, когда применятся в соответствии с правилами, а управление ключами шифрования соответствует корпоративной политике безопасности… Эффективное управление ключами — суть контроля, а необходимость автоматизированного и централизованного управления ключами, интегрированного с существующими в ИТ бизнес-процессами, никем не оспаривается. Даже при шифровании ваших данных внутри облака, важно знать, что вы все еще сохраняете контроль над ключами шифрования. Если вы контролируете ключи, вы контролируете информацию».

НОВОСТИ

ПРОЕКТЫ

В компании «Чумак» внедрили систему «БОСС-Кадровик»

В компании «Чумак» установлена система автоматизации учета персонала и расчета заработной платы «БОСС-Кадровик». Проект стартовал в марте 2012 г. и реализован компанией Инком в рекордно короткие сроки — за 3 месяца.

«Внедрению системы БОСС-Кадровик за столь короткие сроки способствовала инновационная форма реализации в виде удаленного консультирования, а также полное содействие заказчика в процессе работы над проектом. Уже в июле на предприятии «Чумак» была посчитана и выдана заработная плата работникам компании с помощью системы БОСС-Кадровик», — рассказывает Виталий Пустовойт, ведущий консультант отдела внедрения систем управления персоналом компании Инком.

На момент начала внедрения заказчик работал с системой, которая автоматизировала расчет зарплаты, но не покрывала весь спектр потребностей, в частности — расчет зарплаты до заданной суммы оклада. Эта задача выполнялась с помощью таблицы MS Excel.

Проект начинался с обучения, проходившего на территории заказчика, на котором присутствовали все пользователи системы со стороны команды внедрения заказчика и консультанты Инком. Первым этапом внедрения стал перенос данных из существовавшей системы в «БОСС-Кадровик». После завершения работ по настройкам штатного расписания и кадрового учёта команда внедрения приступила к настройке расчета заработной платы, где основным требованием являлось наличие механизма расчета зарплаты до заданной суммы. Проект также содержал и интеграционную часть. Система «БОСС-Кадровик» была интегрирована не только с системой начисления заработной платы с перечислением на банковские карточки, но и с существующей на предприятии ERP-системой «Монолит». В рамках стыковки предусматривалась передача хозяйственных операций (проводок) по начисленной сотрудникам заработной плате в аналитических разрезах.

При использовании материалов ссылка на сайт pcweek.ua обязательна

>>> НАЧАЛО НА С. 8

надежно защищены, либо если они для вас не важны. Аутсорсинг бизнес-процессов, не составляющих «ядро» вашего бизнеса, не является чем-то из ряда вон выходящим. По этой причине облака не несут ничего нового: многие компании уже давно вывели вспомогательные функции в аутсорсинг, оставив под контролем только самые критичные процессы.

Использование специализированных антивирусных решений, созданных для работы в виртуальной среде, повышает уровень защиты облачного сервиса

Если же приложение является критически важным, то переносить его на чужую площадку, будь то ЦОД или распределенная вычислительная архитектура типа облака — несомненный риск, которым нужно управлять. Здесь стоит начать с пересмотра модели доступа к данным: контроль доступа должен осуществляться как можно «ближе» к информации, то есть, на наивысшем уровне абстракции. Другими словами, если в облако попадут только зашифрованные данные, а доступ к ним и их обработка будут происходить с использованием уникальных реквизитов доступа и сильной криптографии, то для заказчика неважно, где физически расположены данные: криптография позаботится об их защите где угодно.

Компания «БМС Консалтинг» предлагает целый ряд решений на базе облачных сервисов для компаний-заказчиков разных размеров. Это решения фильтрации контента, управления инфраструктурой, обеспечения управления безопасностью, мобильными устройствами пользователей от таких производителей, как Symantec, McAfee, AirWatch и MobileIron.

Владимир Удалов: Облачные сервисы, как и любые другие информационные системы, обладают потенциальными уязвимостями, и могут быть атакованы хакерами. Учитывая тот факт, что все более крупные компании размещают свою корпоративную информацию в облаке, в том числе бизнес-критичную, конфиденциальную информацию, можно прогнозировать рост интереса хакеров к облачным сервисам.

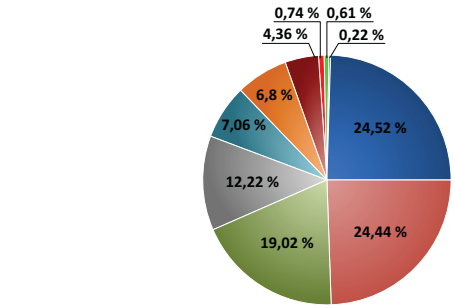
При выборе провайдера и облачных приложений, необходимо руководствоваться бизнес-критичностью тех данных, которые вы планируете размещать в облаке. Так, особо важные и конфиденциальные данные можно хранить внутри компании, менее важные — в публичных облачных сервисах. Это позволяет минимизировать риски и поэтому должно быть прописано на уровне политики безопасности каждой конкретной компании.

Однако при размещении информации в публичном облаке компания не имеет возможности проверить уровень обеспечения безопасности. И даже если провайдеры облачных сервисов допустят своих клиентов к проведению аудита информационной безопасности своих серверов, далеко не у каждого заказчика найдутся специалисты необходимой квалификации.

Таким образом, клиенту остается лишь довольствоваться той информацией о мерах, применяемых для защиты облачного сервиса, которую предоставляет сам провайдер. Сегодня именно на доверии пользователя к облакам и строится их существование. Но в ближайшие годы, скорее всего, появятся компании, которые будут специализироваться на независимом аудите информационной безопасности публичных облачных сервисов. А сертификаты, подтверждающие высокий уровень информационной безопасности, войдут в «джентельменский набор» любого крупного облачного сервиса.

Большинство облачных сервисов базируются на технологии виртуализации. Использование специализированных антивирусных решений, созданных для работы в виртуальной среде, повышает уровень защиты облачного сервиса и помогает добиться правильного баланса между защищенностью и производительностью.

В 2012 г. «Лаборатория Касперского» представила на рынке новое корпоративное защитное решение Kaspersky Security для виртуальных сред. Решение не требует установки антивирусного агента на каждую виртуальную машину, обеспечивая таким образом максимальную защиту виртуальной инфраструктуры без снижения ее производительности. Кроме того, заказчики получают возможность централизованно управлять защитой широкого спектра устройств (включая физические серверы, виртуальные машины и мобильные устройства): при помощи единой консоли Kaspersky Security Center происходит управление политиками, обновлениями и другими задачами по обеспечению ИТ-безопасности. Таким образом, упрощается и повышается прозрачность администрирования, сокращаются затраты и нагрузка на системных администраторов.



Распределение фишинга по типу сайтов. Kaspersky Security Bulletin, май 2012
Источник «Лаборатория Касперского, 2012»

DOCFLOW УКРАЇНА 2012
Все про електронний документообіг та управління бізнес-процесами
Управління електронними та паперовими документами
Організатор: ABBYY
Генеральний медіа-партнер: PCWEEK
Генеральний інтернет-партнер: РБК Україна
Спонсори: Canon, IBA GROUP, Docsvision
Медіа-партнери: Мир денег, it BUSINESS, itpartner, ММ, Коммуникации и связи, Телеком, IT Менеджмент, Банкиръ, Дебет-Кредит, Довідник секретаря та офіс-менеджера, Генеральный директор
19 вересня 2012, Київ
«Український дім», вул. Хрещатик, 2
Для зареєстрованих слухачів відвідування БЕЗКОШТОВНЕ
Час роботи конференції-виставки: з 9:30 до 17:00.
Оргкомітет: тел.(044) 490-9999
факс (044) 490-9461
docflow@abbyy.ua

НЕУДОБНАЯ ПРАВДА О РЕЗЕРВНОМ КОПИРОВАНИИ

ВИТАЛИЙ САВЧЕНКО

В надежде защитить себя от негативных последствий сбоев в ИТ-среде компании тратят значительные средства на разработку плана послеаварийного восстановления. Однако 100%-й уверенности в том, что таким образом они надежно застрахуют себя от неприятностей, у них нет. Резервное копирование и восстановление данных относятся к наиболее важным задачам, тем более что современные компании используют колоссальные объемы информации. Для кого-то ненадежность систем защиты данных может стать неожиданностью, ведь множество организаций инвестировало миллионы в технологии резервного копирования и восстановления данных. Реальная же ситуация такова: нет никакой гарантии, что компании смогут восстановить данные из резервных копий в заданные сроки. В худшем случае восстановить утерянную информацию вообще не удастся. При этом стоимость гарантированного безопасного восстановления каждого байта данных после аварии настолько высока (как в денежном выражении, так и с точки зрения трудозатрат и расходов на инфраструктуру), что многие организации даже не пытаются решить эту задачу. Когда все-таки случается самое худшее, любой результат восстановления будет крайне непредсказуем. Таким образом, компании играют в «русскую рулетку», рискуя своими данными.

Резервное копирование данных остается трудоемким процессом. Тем не менее, выполнять его нужно, иначе вы рискуете безвозвратно потерять ценную информацию. Самый простой способ создания резервных копий подразумевает копирование данных на дополнительное устройство хранения. Однако в рамках ведения бизнеса необходим более серьезный подход.

Компаниям следует инвестировать в инфраструктуру, а также в средства для безопасного хранения, надежного резервного копирования и восстановления данных. Для этого нужно располагать деньгами, временем и сотрудниками, чтобы в случае аварийной ситуации не потерять огромный объем информации. И важно совершенно четко определить, какие именно данные имеют решающее значение для бизнеса. Резервное копирование всего подряд может стать дорогостоящим занятием в пересчете на дополнительное оборудование и требуемый объем дискового пространства. Резервное копирование данных — не простая задача для бизнеса, а кропотливый, сложный и дорогостоящий процесс.

Виртуализация не решает проблем бекапа

Благодаря виртуализации у компаний появилась возможность сделать процессы защиты данных менее ресурсоемкими. При этом значительно снижаются расходы на инфраструктуру, так как для резервного копирования виртуальных машин требуется меньше физических устройств. Существуют инструменты, которые позволяют легко управлять средой виртуального резервирования. Поэтому технология виртуализации становится оптимальным выбором защиты данных.

Итак, технология виртуализации может сделать процесс резервного копирования и восстановления данных более экономичным. Тем не менее, всех задач она не решает. Одним из вечных проблемных вопросов остается тестирование. В физической среде именно ненадлежащее тестирование резервных копий всегда являлось «узким местом» систем защиты данных, из-за которого снижалась эффективность резервного копирования. Конечно, это замечательно, если можно создать резервные копии и восстановить содержимое целых машин и даже данные на уровне отдельных файлов из резервной копии какой-либо машины. Но когда машина повреждена или файлы не читаются, весь процесс бесполезен. Кстати, проблема не только в «полезности» резервной копии.

С точки зрения соблюдения политики компании нет уверенности в том, что план защиты данных будет отвечать всем требованиям. Основная сложность заключается в том, что тестирование восстановления данных зачастую проводится слишком нерегулярно или не на всех машинах. Оно может откладываться либо выполняться частично. Но в современных условиях подобный компромисс неприемлем.

Тестирование — слабое звено

Отсутствие необходимых ресурсов является главным фактором, из-за которого проверка резервных копий, как и многие другие операции, не проводится надлежащим образом. Чтобы корректно протестировать резервную копию, ее следует восстановить, однако это не так просто. В целях экономии резервные копии размещаются, как правило, на сравнительно дешевых системах хранения данных. А они не очень подходят для тестирования на предмет возможности восстановления. Значит, нужна дополнительная инфраструктура. Для тестирования резервных копий можно выделить необходимый объем дискового пространства на имеющемся оборудовании. Но это иногда приводит к дополнительным рискам и в целом отрицательно влияет на рабочую среду в случае сбоя при тестировании. Есть и другой выход из ситуации — построить совершенно новую инфраструктуру. И тот и другой варианты отнимут полезное машинное время, а также потребуют дополнительных расходов и трудозатрат, которые организация могла бы с пользой потратить на что-нибудь еще. Даже если компания может выделить средства из своего бюджета на дополнительную инфраструктуру, для проверки резервных копий придется израсходовать много времени и дополнительных ресурсов.

Таким образом, тестирование сводится, как было сказано, к простой расстановке приоритетов. Многие организации с ограниченными рабочими ресурсами рассматривают тестирование и верификацию для событий, которые могут никогда не произойти, как низкоприоритетные задачи по сравнению с неотложными бизнес-процессами. Даже если тестирование все-таки проводится, организациям все равно трудно определить, когда данные стали невосстановимыми, поскольку нет возможности восстановить каждую резервную копию. Так как данные сейчас крайне важны для бизнеса, подобные задачи приобретают первостепенное значение.

Необычное решение

Для устранения этой дилеммы существует решение, и оно лежит, как ни странно, в области виртуализации. Благодаря исследованиям в сфере безопасности стали очевидны преимущества виртуализации при создании жизнеспособных, изолированных тестовых сред. В них оценивается эффективность средств защиты от вредоносного ПО и других угроз без риска для всей инфраструктуры. Организации могут создавать изолированную среду для тестирования резервных копий. Такая временная среда быстро формируется с привлечением любых свободных рабочих ресурсов при использовании среды для резервного копирования, что избавляет от необходимости инвестировать в новую инфраструктуру.

Поскольку единственная цель этой среды — проверка корректности восстановления резервных копий, то нагрузка на инфраструктуру минимальна и краткосрочна. При этом требуются некоторые вычислительные ресурсы, которые обычно используются в рабочем окружении. Поскольку виртуальная машина запускается непосредственно из сжатой резервной копии, нужно будет опубликовать содержимое резервных файлов на хосте ESX(i) во временной виртуальной среде для тестирования. В итоге машины можно тестировать быстро и безопасно, используя только часть инфраструктуры. Теперь тестирование резервной копии каждого сервера перестанет казаться несбыточной мечтой.

До сих пор тестовое восстановление всех резервных копий для многих оставалось недосягаемой целью. Но теперь все изменилось. Компании либо приспосабливаются к меняющемуся технологическому климату, либо искушают судьбу и ждут неприятностей, используя устаревшие подходы к резервному копированию и восстановлению данных. По мере того как виртуализация все чаще признается стандартом в области защиты данных, тестирование и верификация с использованием соответствующих инструментов становятся проще. А это дает организациям возможность сохранять конкурентоспособность.

Автор статьи — руководитель группы системных инженеров Veeam Software в России и СНГ

НОВОСТИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Треть украинских пользователей применяют примитивные пароли

Исследование, проведенное в преддверии запуска Kaspersky Internet Security 2013 по заказу «Лаборатории Касперского» компанией O+K Research в 25 странах мира, показывает, что угрозу простых паролей пользователи пока не осознали, данные 34% опрошенных практически не защищены.

Согласно результатам опроса, весьма часто используются вовсе небезопасные пароли, которые легко подобрать даже без использования специальных методик. Речь идет о дате рождения (16%), middle name (3%) или кличке домашнего животного (6%) — эту и другую подобную информацию могут узнать не только близкие друзья и родственники. Ее без особого труда можно найти в Интернете, например, в социальных сетях. Злоумышленнику нужно лишь проявить немного сообразительности. Еще 15% опрошенных используют сочетание цифр «123456» или похожее, а 6% — слово «пароль». Такая «защита», равно как и другие пароли, основанные на простых словах, может быть легко вскрыта за короткое время. Еще одна проблема безопасности, на которую пользователи редко обращают внимание, — использование повторяющихся паролей. Такой подход позволяет не перегружать память большим количеством цифробуквенных комбинаций, но если один пароль попадет в руки киберпреступников, они смогут получить доступ сразу к нескольким сервисам или программам. По данным O+K Research в Украине 6% опрошенных устанавливают один пароль на все учетные записи, а 34% — используют всего лишь несколько паролей. С учетом того, что треть украинских участников исследования (65%) используют 5 и более защищенных паролем сервисов и приложений, можно представить себе масштаб «дыры» в защите.

ИТ-БИЗНЕС

HP планирует возобновить производство смартфонов

HP может предпринять уже третью в своей истории попытку по выпуску смартфонов. С таким заявлением выступила глава компании Мег Уитман. «В перспективе мы намерены возобновить разработку и производство смартфонов, которые во многих странах являются первым вычислительным устройством. Мы — компания, занимающаяся производством вычислительных устройств и должны воспользоваться этим фактором»,— сказала она в интервью американскому телеканалу Fox Business Network. До этого HP выпускала целый ряд смартфонов и КПК серии iPaq на базе ОС Windows Mobile, в первую очередь позиционируемых для использования корпоративным сектором, но, по оценке IDC, доля устройств такого типа на рынке смартфонов составила лишь 0,1%.

После приобретения Palm в 2010 г. HP свернула производство Windows Mobile-смартфонов и выпустила на рынок планшет и смартфоны уже под управлением webOS.

С приобретением Palm в HP рассчитывали на ее основной актив — webOS, на базе которой были выпущены планшет HP TouchPad, а также смартфоны Pre и Veer. Представленный в феврале 2011 г. TouchPad был не лучшим образом встречен потребителями. Более того — с ним произошла скандальная история, когда популярная в США розничная сеть Best Buy вообще сняла этот планшет с продаж, посчитав, что он загромождает ее склады, где находилось 270 тыс. нереализованных устройств (реализовано было лишь 25 тыс. планшетов HP). Смартфоны Pre и Veer также продавались не лучшим образом.

В конце 2011 г., после череды слухов в прессе о дальнейшей судьбе webOS корпорация объявила, что откроет к сентябрю 2012 г. исходный код операционной системы webOS и продолжит усовершенствование этой мобильной ОС уже в ее новом статусе. А в середине августа этого года HP начал предпринимать новые шаги по реформированию своего мобильного бизнеса. Так, компания выделила бизнес по разработке webOS в самостоятельную компанию GRAM, по-прежнему целиком принадлежащую HP, но имеющую право привлекать внешние инвестиции.

Практически одновременно с созданием GRAM из опубликованной интернет-ресурсом The Verge служебной записки руководителя группы устройств печати и персональных систем (Printing and Personal Systems Group) Тодда Бредли, подлинность которой подтвердил представитель HP, стало известно о формировании нового подразделения в составе HP по выпуску мобильных устройств, получившего название Mobility Global Business Unit.

Это подразделение будет разрабатывать планшеты, а также заниматься «дополнительными сегментами и категориями», где, как полагает компания, тоже можно будет предложить потребителю что-то ценное. Возглавит новое подразделение Альберто Торрес, ранее отвечавший за развитие MeeGo в компании Nokia. В документе сказано, что Торрес, входящий в совет директоров компаний Bang & Olufsen и Opera Software, приступит к выполнению обязанностей руководителя нового подразделения HP в сентябре.

При использовании материалов ссылка на сайт pcweek.ua обязательна

20-24 ОКТЯБРЯ, ГРУЗИЯ, БАТУМИ

«ЛУЧШИЕ IT-ПРОЕКТЫ»

LIVE! X ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ «АВТОМАТИЗАЦИЯ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ»

Генеральный спонсор: IBM

Спонсор: bpm

Партнер: Украинский процессинговый центр

Генеральный медиа-партнер: PCWEEK

Медиа-партнеры: itpartner, IT Менеджмента, Карт Бланш, Bankstore.com.ua, Prostobankir.com.ua

+38 057 760-13-67
+38 067 570-08-92

www.csltd.com.ua
conf@csltd.com.ua

ПРОГНОЗИРУЯ БУДУЩЕЕ КОРПОРАТИВНОГО ИТ-РЫНКА

АЛЛАН АЛТЕР, ДЖИН ХАРРИС

ПЕРСПЕКТИВЫ

Не думайте что будущее легко предсказуемо и будет готовым к восприятию передовых технологий. Не стройте предположений, что ИТ- и бизнес-платформы будущего станут развитием используемых сегодня. Вместо этого задайте себе эти десять вопросов, чтобы узнать, что будущее может потребовать от вашего ИТ-департамента.

Если бы вы могли выбрать какую-либо одну бизнес-функцию, которую надо перестроить в первую очередь, что бы это было? Консалтинговая компания Accenture, в которой я работаю, задала этот провокационный вопрос 152 ИТ-менеджерам и 164 другим руководителям в четырех странах. В большинстве случаев (особенно среди специалистов по технологиям) было указано упорядочение ИТ. Половина респондентов этого опроса также отметили, что они или уже переделывают корпоративную ИТ-инфраструктуру, или собираются этим заняться в ближайшее время.

Менеджеры стремятся к реорганизации своих ИТ-департаментов, но как будут выглядеть они завтра, после завершения реорганизации? Какие у них будут обязанности, роли и приоритеты?

Большинство менеджеров все еще ломает над этим головы. 68% из них не знает, как будут выглядеть функции ИТ-службы к 2016 г. Еще больше руководителей не имеют ясного представления о будущей роли ИТ-директора.

Кто может их винить? Существует огромное количество вопросов о том, как облачные вычисления, мобильные компьютеры и потребительские технологии повлияют на ИТ-департаменты.

Неопределенность выходит за рамки технологий. ИТ-организации находятся под действием тех же непостоянных социальных, политических и экономических сил, которые влияют и на весь деловой мир. Планирование развития ИТ, исходя из предсказуемого, интегрированного и технически обеспеченного будущего и без принятия во внимание тех изменений, которые может потребовать бизнес в результате совокупного действия социальных, политических и экономических факторов, как минимум — наивность, а как максимум — опасная близорукость.

Глобальная интеграция и экономическое сотрудничество не являются чем-то навсегда заданным свыше. Мы надеемся на продолжение этих процессов, но нам может и не повезти, особенно если масштаб современного экономического кризиса и геополитической напряженности продолжит расти и вызовет дальнейшее усиление раскола в мире. Это способно заставить компании начать сокращение расходов на привлечение иностранных ИТ-специалистов и контакты с новыми партнерами и вынудить руководителей реструктурировать бизнес-процессы и ИТ-операции.

Рассмотрим, например, потребительские технологии. Они могут продолжить изменять ежедневную жизнь и ИТ-ожидания. Или опасения за приватность и безопасность данных заставят частных и корпоративных пользователей проявлять большую осторожность в работе с Интернетом. Сегодня трудно представить себе мир без Интернета, но отдельные руководители пытаются это сделать. 27% менеджеров, которых мы опросили, ожидают начала поиска альтернатив для Всемирной сети к 2016 г.

Другая неопределенность: насколько сильно конкуренция с транснациональными корпорациями, действующими в развивающихся странах, повлияет на бизнес-сообщество и принятые в нем способы управления ИТ.

42% ИТ-менеджеров в ходе нашего опроса высказали мнение, что глобальные корпорации, скорее всего, смогут значительно сократить свои расходы на ИТ. Этот факт наверняка привлечет внимание вашего финансового директора.

Нет ничего удивительного, что в подобных обстоятельствах так тяжело представить себе будущее ИТ-департамента и самого ИТ-директора. Развитие может пойти совершенно разными путями, и трудно предсказать, как это повлияет на приоритеты и операции ИТ-служб.

Как может ваша команда ИТ-руководителей начать планировать новую структуру ИТ-подразделения компании? Ответ один — работая вместе с другими менеджерами над выработкой представления о будущих способах ведения бизнеса. Они должны обдумать все факторы, оказывающие давление на вашу ИТ-организацию, и взвесить разнообразные решения, которые нужно будет предпринять ИТ-руководителям.

Следующие 10 вопросов помогут руководителям связать возможные варианты развития событий и базовые ИТ-решения, касающиеся организационной структуры, ИТ-инвестиций, компетенций персонала и новых технологий (таких как облачные вычисления). Некоторые из них фокусируются на основных принципах участия ИТ в производственной деятельности. Другие больше относятся к проблеме управления ИТ-структурой в будущем. Вместе они помогут вам увидеть возможности реорганизации вашей ИТ-службы, предвидеть изменения и спроектировать более жизнеспособную ИТ-систему.

1. ПОЧЕМУ ИТ БУДЕТ ИМЕТЬ ЗНАЧЕНИЕ ДЛЯ МОЕЙ КОМПАНИИ?

Компании могут добиваться с помощью ИТ больших успехов, чем когда-либо ранее, но они не так часто прислушиваются к мнению своих ИТ-подразделений при выборе и внедрении технологий. Уточнение цели ИТ-подразделения поможет сфокусировать усилия по его реконструкции.

Если будущее останется глобально взаимосвязанным и предельно конкурентным, ИТ-подразделения должны помочь лидерам индустрии удержать лидерство, предлагая инновации и точную аналитику. Корпоративная ИТ-инфраструктура начинает выступать в качестве глобально управляемого актива. Но даже если мир двинется в сторону большей фрагментарности, разрозненности и уязвимости, ИТ-подразделение все еще способно окупить затраты на свое содержание — помогая в реструктуризации бизнеса, снижая затраты компании и обеспечивая непрерывность операций на время реформ.

2. КАК БУДЕТ ВЫГЛЯДЕТЬ НАША СЛУЖБА ИТ, ЕСЛИ МЫ СМОЖЕМ ПЕРЕСТРОИТЬ ЕЕ С НУЛЯ?

Будет ли какая-либо компания при перепроектировании своей ИТ-инфраструктуры пытаться сохранить ее в предыдущем виде? Скорее всего, нет. На что же была бы похожа ИТ-служба, если бы руководство компании, включая ИТ-директора, могло бы действовать без каких либо ограничений?

Подумайте об организационной структуре, наиболее подходящей для вариантов развития, которые вы рассматриваете. В зависимости от юридических, политических и технических аспектов это может быть отлаженная глобально действующая ИТ-структура, управляющая оказанием услуг по модели «облака и аутсорсинг», или децентрализованный ИТ-департамент с мощными локальными ИТ-подразделениями. В случае сохранения угрозы киберпреступности может также потребоваться усиление контроля над обеспечением информационной безопасности.

3. КАК НАШИ ИТ-МЕНЕДЖЕРЫ И ДРУГИЕ РУКОВОДИТЕЛИ БУДУТ ОБСУЖДАТЬ И ОДОБРЯТЬ РЕШЕНИЯ В ОБЛАСТИ ТЕХНОЛОГИЙ?

Цепочка принятия решений в ИТ становится все длиннее. Социальные медиа и аналитики все больше втягивают в принятие ИТ-решений ведущих специалистов по маркетингу. Компании нанимают директоров по инновациям и цифровой обработке. Сотрудники спокойно принимают ИТ-решения, касающиеся их самих.

В этой ситуации руководителям надо сконцентрироваться на управлении, а не вступать в борьбу за власть. Этот вопрос помогает понять, какие ИТ-решения должны приниматься на глобальном или региональном уровнях, а какие лучше принимать самим сотрудникам и руководителям среднего звена. Это также поможет ответить на вопросы о роли ИТ-директора, а также о необходимости контроля ИТ-департамента со стороны специально назначенного чиновника — директора по стратегии или директора по рискам.

4. КАК ВЫ ОБЕСПЕЧИТЕ ДОСТУПНОСТЬ СВОИХ ДАННЫХ ВЕЗДЕ, ГДЕ ОНИ НЕОБХОДИМЫ?

В эпоху смартфонов и аналитики люди ожидают постоянного доступа ко всем типам данных с любого устройства. Не имеет значения, идет ли речь о структурированных результатах транзакций или неструктурированных массивах видео и аудио, огромных базах данных или небольшом объеме критически важной информации. Задача ИТ состоит в налаживании взаимодействия старой и новой архитектур, чтобы обеспечить безопасную и надежную доставку полезных сведений всем, кому они необходимы.

При любых вариантах развития эти ожидания могут осложниться возможными проблемами, такими как юридические ограничения, угрозы безопасности и перебои с услугами. Но даже в этих обстоятельствах необходимо найти способ максимально приблизиться к идеальному стандарту полной доступности информации и результатов ее анализа.

5. МЫ ВЫИГРЫВАЕМ ИЛИ ПРОИГРЫВАЕМ БИТВУ ЗА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ?

Будущее ИТ в значительной мере будет определяться уровнем серьезности угроз со стороны киберпреступности. Смогут ли компании и правительства справиться с этой проблемой с помощью технологических новинок или международного сотрудничества? Если да, то проблемы кибербезопасности начнут отходить на второй план.

Но что если киберпреступность (или даже кибервойна) выйдет из-под контроля? Традиционные методы ведения бизнеса компаниями и их клиентами на основе нынешних ИТ-операций уйдут в прошлое. Если ситуация действительно ухудшится, компаниям придется пересмотреть и значительно ограничить большинство своих операций, использующих Интернет. ИТ-департаменты сфокусируются на поиске альтернатив современной, основанной на Интернете сетевой инфраструктуре для минимизации возможного ущерба.

6. КАКОЙ ТИП ОБЛАЧНЫХ СЕРВИСОВ БУДЕТ ПРЕОБЛАДАТЬ?

Одни варианты развития событий благосклонны к облачным сервисам, другие — нет. Предсказуемый, глобально взаимосвязанный, не регулируемый принудительно мир создает благоприятную почву для облачных вычислений и услуг на платформе публичного облака. При наличии высокоскоростного широкополосного доступа в Интернет не остается никаких препятствий на пути повсеместного использования бизнесом глобальных облачных сервисов.

Однако в случае предъявления жестких требований к способам хранения и обработки данных, применения протекционистской экономической политики и национальных аналогов Интернета компании могут быть вынуждены отказаться от глобальных облачных сервисов и перейти на работу с частным облаком и локальными провайдерами облачных технологий. И хотя крупные облачные компании могут позволить себе серьезные инвестиции в первоклассные технологии обеспечения безопасной и надежной работы, это не будет иметь никакого значения, если их клиенты не смогут наладить надежно защищенный канал обмена данными с публичными облаками.

7. НАСКОЛЬКО СРОЧНО МЫ ДОЛЖНЫ ПРИНИМАТЬ В РАСЧЕТ ТЕХНОЛОГИИ, РАССЧИТАННЫЕ НА ШИРОКОЕ ПОТРЕБЛЕНИЕ?

Потребительские ИТ-продукты возникают на пересечении бизнеса, инноваций и стиля жизни, и это делает их непредсказуемым феноменом для ИТ-структур. Трудно представить себе, что будут предлагать через пять лет социальные сети и смартфоны, и еще труднее оценить, какие новые приложения окажутся востребованными сотрудниками компаний.

Тем не менее люди, отвечающие в корпорациях за планирование развития ИТ, могут уже сейчас приступить к изучению возможных последствий распространения потребительских ИТ, включая необходимость найма новых сотрудников и тестирование новых технологических трендов. Такие факторы, как стоимость, наличие широкополосного доступа, технологии доступа к сети с мобильных устройств, скорость внедрения инноваций, доступ к потребительским приложениям и данным из других стран, цензура и уровень доверия к ИТ-безопасности, будут оказывать влияние на предложение потребительских ИТ-товаров и услуг и спрос на них как на рынке, так и на рабочих местах.

8. В КАКИХ ИТ-КОМПЕТЕНЦИЯХ НАМ НУЖНО ПРЕУСПЕТЬ И ГДЕ ОНИ БУДУТ НАМ НЕОБХОДИМЫ?

Задайте этот вопрос после того, как ответите на остальные. Начните с разделения работ по ИТ на управление, руководство, проектирование, разработку, анализ и операции. Затем спросите, что необходимо сделать и какие компетенции для этого потребуются.

Например, чем необходимо управлять? Провайдерами услуг? Инфраструктурой? Где они управляются — глобально или локально? Или рассмотрим проектирование ИТ: какие компетенции будут нужны архитекторам и сетевым инженерам для проектирования гибридной инфраструктуры «облако — сервер» (специальный тип архитектуры, объединяющий взаимодействующие друг с другом ресурсы, развернутые одновременно в традиционной сети on-premise и в облаке) или мигрирования в сеть, созданную на закрытых стандартах? Какой опыт лучше всего подготавливает руководителя к тому, чтобы поощрять инновации: руководство централизованной или децентрализованной структурой или управление кризисами в области информационной безопасности?

9. ОТКУДА ПОЯВЯТСЯ ИТ-ТАЛАНТЫ?

Сегодня предприниматели предполагают, что могут легко отыскать необходимых ИТ-профессионалов в странах с низким уровнем жизни и быстро переместить их через границы. Но что если глобализация приостановится, новые правила не позволят вам более выкачивать ИТ-специалистов из других стран, а дистанционное сотрудничество сильно осложнится? Что случится, если компании не смогут найти местных исполнителей, когда это диктуется интересами национальной безопасности или требованиями культурологического характера? Если компании не имеют разрешения на приглашение иностранных талантов или не могут использовать офшорное программирование, они будут вынуждены увеличивать инвестиции в подготовку национальных кадров или в перемещение своих сотрудников с места на место.

ПРОДОЛЖЕНИЕ НА С.20>>>

При использовании материалов ссылка на сайт pcweek.ua обязательна

- Защищает конфиденциальные данные и проверяет соблюдение политик
- Защищает планшеты, не мешая работать
- Высококлассная защита корпоративного класса от утечки данных

Symantec
Data Loss Prevention for Tablets

Защита iPad®, обеспечиваемая лидером в области предотвращения утечки данных

Каждый день ваши сотрудники приносят все больше устройств iPad на работу и подключают к корпоративной сети, где они имеют доступ к конфиденциальной информации компании. К счастью, у нас есть продукт Symantec Data Loss Prevention for Tablets, обеспечивающий надежную защиту от утечки данных, поэтому ваши сотрудники смогут использовать устройства iPad, не подвергая риску конфиденциальные данные организации. В случае неправильной работы с конфиденциальными данными или нарушения установленных политик создаются мгновенные предупреждения. Это просто, необременительно и, главное, эффективно. Загрузите справочный документ «DLP for Tablets: An Intelligent Security Decision» с веб-сайта go.symantec.com/dlp

Уверенность в мире информационных технологий. Symantec

Copyright © 2012 Symantec Corporation. Все права защищены. Symantec, логотип Symantec и логотип с галочкой являются товарными знаками или зарегистрированными товарными знаками Symantec Corporation или ее дочерних компаний в США и других странах. iPad является товарным знаком Apple Inc., зарегистрированным в США и других странах. Другие названия могут являться товарными знаками соответствующих владельцев.

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ: 10 ИЗМЕНЕНИЙ К 2020 г.

ДЖЕК КЛАРК

В данный момент мы пребываем в начальной стадии развития облачных вычислений. Многие организации делают лишь первые, неуверенные шаги. Но к 2020 г. облако станет главной и непременной частью вычислительной инфраструктуры предприятия. Вероятно, через восемь лет многие задачи в облаке будут обрабатывать малопотребляющие процессоры, работающие в высокоавтоматизированных ЦОДах и поддерживающие тесно интегрированную, масштабируемую архитектуру ПО.

Аналитическая группа Forrester прогнозирует, что мировой рынок облачных вычислений вырастет с 35 млрд долл. в 2011 г. до примерно 150 млрд долл. в 2020-м. Облака станут важнейшим элементом ИТ-инфраструктуры многих организаций.

Помимо этого будут развиваться поддерживающие облака технологии. Быстрое увеличение вычислительной мощности сделает облачные проекты еще дешевле, поскольку технологии, реализуемые в настоящее время только на суперкомпьютерах, станут массовыми.

И конечно, к 2020 г. в организациях произойдет смена поколений. Появятся CIO, выросшие во времена использования облачных инструментов. Они будут в гораздо большей степени готовы к применению облаков в масштабе предприятия.

С учетом названных тенденций мы назовем 10 кардинальных отличий облаков 2020 г. от сегодняшних. Именно на них указали эксперты.

1. ПО теряет связь с аппаратурой

Джон Менли, директор лаборатории HP Automated Infrastructure, считает, что ПО отрывается от оборудования. Все новые и новые технологии будут предоставляться в виде сервиса. «Облака окончательно превратят вычисления в невидимые», — заявил он.

В результате, если в 2020 г. вы попросите CIO нарисовать карту инфраструктуры, он не сможет этого сделать, сказал Дэвид Меррилл, главный экономист Hitachi Data Systems. «Вот мои партнеры-провайдеры», — скажет он. А изобразить схему размещения своей инфраструктуры не сумеет.

Это связано с тем, что она будет находиться в «абстрактном пространстве», где ПО пишется таким образом, что перед взаимодействием с оборудованием оно проходит через ряд фильтров. Это означает, что клиентские приложения или приложения, созданные поверх «платформы как сервиса», будут инвариантны к аппаратному обеспечению.

2. Модульное ПО

Чтобы воспользоваться огромным парком аппаратуры, доступной через облака, каждое приложение в отдельности должно стать объемнее и сложнее, поскольку оно пишется в расчете на использование эффекта масштаба. С ростом размеров и сложности программ акцент в процессе разработки ПО будет смещаться в сторону модульного ПО. Востребованными станут крупные приложения, компоненты которых могут модифицироваться без прекращения работы программы. Соответственно облачные приложения потребуют от программистов нового склада мышления, особенно в случаях взаимодействия с несколькими облаками.

«К ПО необходимо подходить по-разному», — отметил Менли. Он считает, что в 2020 г. одной из главных проблем станет управление интегрированными сервисами. Это связано с тем, что приложения будут не только размещаться в облаке, но и обращаться к другим облакам и к приложениям, размещенным в ЦОДах различных компаний. Иными словами, различные части приложений находятся у сервис-провайдеров и вокруг них. По мнению Менли, проблема будет заключаться в том, чтобы добиться хорошего соглашения об уровне обслуживания.

3. Социальное ПО

Наряду с модульной архитектурой ПО может приобрести особенности, характерные сейчас для приложений социальных сетей вроде Facebook, заявил Меррилл. При необходимости программы смогут автоматически создавать кратковременные связи с элементами оборудования и ПО.

«Это будет эволюция в направлении социальных сетей, — считает Меррилл. — У вас будет инфраструктура. Она будет выглядеть как облако, но мы спроектируем ее так, чтобы СУБД «нравился» сервер или массив хранения».

Иначе говоря, инфраструктура и ПО ЦОДа будут формироваться вокруг решаемой задачи, а не наоборот. Разработчикам больше не придется заботиться о выделении объема хранения, сервера и коммутатора, сказал Меррилл. Все это будет происходить автоматически.

4. Оборудование потребительского класса правит бал

К 2020 г. будет полным ходом осуществляться переход на недорогое оборудование. Такие схемы, как Open Compute Project, выйдут за пределы ЦОДов Facebook и Amazon Web Services и станут внедряться и небольшими компаниями. «Серверы и системы хранения будут сменными, выдвигающимися на салазках», — заметил Фрэнк Френковски, директор Facebook по техническим операциям и председатель правления проекта Open Compute Project.

Если разделить инфраструктуру на базовые компоненты, можно быстро производить замены и апгрейды, сказал он. Лучше всего инфраструктура на оборудовании потребительского класса подходит крупным компаниям, имеющим большие ЦОДы. «Я бы сказал, что с нынешнего времени и до 2020 г. наиболее быстро растущим сектором рынка станут облачные сервис-провайдеры», — заявил Френковски.

5. Малопотребляющие процессоры и более дешевые облака

Примерно год отделяет нас от появления на рынке малопотребляющих процессоров ARM с 64-разрядными возможностями. И когда это произойдет, их начнут массово использовать. Для RISC-процессоров будет разработано корпоративное ПО, позволяющее компаниям применять в своих ЦОДах экономно расходующие энергию процессоры и тем самым на порядок снизить затраты на электричество.

HP создала в рамках проекта Moonshot пилотную серверную платформу Redstone, чтобы посмотреть, как клиенты воспримут процессоры ARM. A Dell уже многие годы продает серверы заказной конфигурации на процессорах ARM крупнейшим облачным клиентам через свою группу Data Center Solutions.

Весьма вероятно, что к 2020 г. малопотребляющие процессоры можно будет встретить повсеместно. И не только процессоры ARM. Intel, сознавая нависшую над ней угрозу, напряженно трудится над снижением энергопотребления процессоров Atom. Правда, в основном ее усилия в данной области нацелены на мобильные устройства, а не на серверы. Facebook считает, что распространение процессоров ARM начнется с устройств хранения, а затем охватит серверы.

«Я думаю, это окажет огромное влияние на объем выполняемой полезной работы в расчете на доллар», — заметил Френковски. Это поможет облачным провайдерам, таким как Amazon Web Services, снизить расходы на электричество. Более того, если они участвуют в войне цен с конкурентами, то, вероятно, поделятся по крайней мере частью сэкономленных средств с разработчиками, снизив цены на свои сервисы.

6. Более быстрые внутренние соединения

Сочетание потребностей в широко распределенных приложениях и наращивании числа ядер в высокопроизводительных процессорах приведет к появлению в ЦОДах сверхскоростных внутренних соединений. Как предсказывает Джозеф Регер, главный технолог Fujitsu Technology Solutions, можно ожидать, что к 2020 г. коммуникации в ЦОДах «будут осуществляться со скоростью нескольких сотен гигабит в секунду».

По мнению Регера, произойдет «очень быстрое превращение» технологий скоростных внутренних соединений в массовый товар, что приведет к появлению дешевых и быстрых соединений. Это позволит ускорить передачу информации в ЦОДах и снизить стоимость передачи. Благодаря этому компании смогут создавать более крупные приложения, пересылающие больше данных (их называют «болтливыми»). Перед разработчиками откроется возможность написания более интеллектуальных, автоматизированных и сложных программ.

7. ЦОДы превращаются в экосистемы

Облачный ЦОД будет «во многом напоминать дышащий живой организм, принимающий различные состояния», — считает Регер. Сочетание абстрагированного от аппаратуры ПО и ставшего массовым товаром оборудования сделает ЦОДы похожими на экосистемы. Система более высокого порядка будет управлять оборудованием из одной точки, возможности ЦОДа будут расширяться и сужаться в зависимости от нагрузки.

В результате автоматизации простых задач, таких как ремонт и обновление оборудования, ЦОД «станет больше напоминать биологическую систему», заметил он, в том смысле, что изменения и исправления будут вноситься автоматически.

8. Облака консолидируют

Интернет поощряет большие масштабы. А поскольку в действующие облака вложены огромные капитальные средства, весьма вероятно, что на рынке облачных провайдеров произойдет некоторая консолидация.

Острая конкуренция между несколькими крупными провайдерами может оказаться полезной, поскольку заставит каждого из них экспериментировать с радикально новыми технологиями. Например, в стремлении снизить затраты на внутреннюю сеть и повысить коэффициент ее использования Google перевела недавно всю свою внутреннюю сеть на управление посредством ПО в соответствии со стандартом OpenFlow. Когда этот стандарт получит широкое распространение, он вызовет переворот в отрасли.

Менли считает, что получат развитие различные облака, предназначенные для конкретных целей: «Установится разнообразие. Думаю, монополия могла бы сложиться, если бы появилась инфраструктура, способная в достаточной мере соответствовать всем нефункциональным инфраструктурным требованиям конечных сервисов».

9. Смена поколений

К 2020 г. в компаниях появится новое поколение CIO, выросшее после появления облаков и начала предоставления ИТ в виде сервисов. Они будут ожидать, что все доступно в качестве сервисов, сказал Меррилл: «Наша модель потребления меняется, будучи проблемой поколений. У нас действуют архаичные, основанные на налогах и бухучете правила, препятствующие инновациям». И новое поколение может полностью изменить порядок оплаты услуг ИТ компаниями, считает Меррилл.

10. Возникнет стратификация облаков

Сегодня облака различаются в зависимости от того, какие услуги они предоставляют: инфраструктура как сервис, платформа как сервис или ПО как сервис. А к 2020 г. появятся более специализированные облака.

Согласно Forrester, к 2020 г. можно ожидать появления инструментов промежуточной виртуализации (middle virtualisation tools) и динамических сервисов аутсорсинга бизнес-процессов, а также еще целого ряда труднопроизносимых аббревиатур. Наряду с несколькими крупными провайдерами, предлагающими простые технологии, такие как хранение и вычисления, возникнет широкая сеть провайдеров специализированных облачных сервисов. Они позволят компаниям переносить в облака задачи, которые иначе пришлось бы решать с помощью весьма специфических (и, как правило, очень дорогих) приложений.

Меррилл считает, что облака, как и любые полезные вещи, будут дифференцироваться в зависимости от возможностей их инфраструктуры и разделятся на неизвестные ранее классы. «Подобно тому, как энергию вырабатывают электростанции на угле и природном газе, атомные и гидроэлектростанции, так и тут появятся различия, — сказал он. — Экономика, по моему мнению, способствует дифференциации и категоризации».

>>> НАЧАЛО НА С. 18

Больше компаний станут сотрудничать с университетами для выпуска специалистов, готовых к практической работе.

10. КАК ИЗМЕНЯТСЯ НАШИ ПРИОРИТЕТЫ В РАСХОДАХ?

Отступите на шаг назад и оцените заново, что каждый вариант развития означает для вашего бюджета. Спросите себя — куда при каждом из анализируемых вариантов будущего придется вкладывать деньги для достижения бизнес-целей, решения операционных задач и выполнения юридических требований. Будут ли это инвестиции в инфраструктуру, разработку приложений, сервисы или персонал? Или это будет некоторая комбинация из названных опций? Кроме того, можно ли как-то сократить расходы — например, перейдя на более дешевые опции или отказавшись от решения каких-либо задач? В некоторых вариантах будущего сокращение расходов на ИТ или предоставление сотрудникам и менеджерам прямого контроля над расходами в области ИТ станет особенно важным приоритетом. Мир часто меняется в непредсказуемом и неожиданном направлении, и изменениям подвергаются не только технологии. Безальтернативное планирование развития вашей ИТ-инфраструктуры в будущем без учета возможных вариантов представляется чрезвычайно опасным подходом.

При использовании материалов ссылка на сайт pcweek.ua обязательна

БИЗНЕС НА АККУМУЛЯТОРАХ

ИНТЕРВЬЮ

ОЛЕГ ПИЛИПЕНКО

Компания «Дробак» известна в Украине как один из крупнейших поставщиков зарядных устройств и аккумуляторов для ноутбуков и портативной техники. Подобно многим американским и европейским вендорам, OEM-заказы на производство предприятие размещает в Китае. О специфике рынка аккумуляторных батарей, тонкостях производственного цикла и становлении бизнеса компании «Дробак» рассказывает ее генеральный директор Александр Вовк.

PCWeek/UE: Давно ли представлена на рынке компания «Дробак»? Каким бизнесом вы занимались на старте? Что побудило вас сфокусироваться на аккумуляторах для мобильных устройств?

АЛЕКСАНДР ВОВК: Компания «Дробак» основана в 2008 г. как интернет-магазин по продаже ноутбуков. Однако с наступлением кризиса мы решили диверсифицировать род своей деятельности и освоить новую рыночную нишу, которая тогда была свободной. К концу 2008-го мы осуществили первые поставки аккумуляторных батарей в Украину. Уже в 2009 г. начали вести переговоры с известным заводом в Китае о выпуске аккумуляторов для ноутбуков под собственной торговой маркой. В результате мы подписали договор на производство OEM-продукции, и уже в 2010 г. в Украину прибыла первая партия аккумуляторов для ноутбуков под маркой «Дробак».

Первые пробные поставки так называемых универсальных мобильных батарей (УМБ) были сделаны еще в конце лета 2011-го. Мы не знали, как на них отреагирует рынок, но решили сделать ставку на широкий модельный ряд и не прогадали. Сегодня линейка УМБ — один из лидеров продаж.

PCWeek/UE: Как построен производственный цикл вашей компании? Где находится отдел исследований и разработок?

А.В.: Вся продукция, которая поставляется в Украину под нашей торговой маркой, изготавливается в КНР. Производственные мощности компании расположены в китайской провинции Шеньчжэнь.

Очевидно, что спрос на аккумулятор для новой модели ноутбука появляется лишь через 3-6 месяцев после выпуска на рынок самого лэптопа. Этот период мы используем для тщательного тестирования новой модели батареи. После того, как завод делает пробные модели, их отправляют в Киев для проверки и выявления возможных недостатков. Только после всесторонней «обкатки» мы передаем заказ на серийное производство новинки.

PCWeek/UE: Какой диапазон ноутбуков в процентном выражении покрывает ваш модельный ряд аккумуляторов (без учета УМБ)? Вы ориентируетесь на любые лэптопы, включая нетбуки?

А.В.: С уверенностью можно сказать, что ассортимент предлагаемых нами аккумуляторов на сегодняшний день покрывает 95% моделей ноутбуков, представленных на украинском рынке. Оставшиеся 5% — это те модели ноутбуков, которые выпущены совсем недавно, а также лэптопы, возраст которых превышает 6 и более лет. Мы поставляем батареи как для ноутбуков, так и нетбуков.

PCWeek/UE: Есть ли возможность поставлять батареи для «экзотических» моделей ноутбуков? Если да, то насколько такая услуга повышает цену товара для заказчика?

А.В.: Наша компания уже давно практикует поставку аккумуляторных батарей под заказ для своих партнеров. Но если речь идет о редких моделях батарей, возможность их производства будет оцениваться, исходя из экономических показателей. С другой стороны, сегодня в нашем ассортименте можно найти аккумуляторы таких брендов, как Clevo, Mitac, Gateway, BENQ. Они мало распространены в Украине, однако пользуются стабильным спросом среди заказчиков.

PCWeek/UE: Перечислите наиболее важные направления вашего бизнеса. Какой процент в обороте занимает каждое из направлений?

А.В.: Аккумуляторы для ноутбуков являются основным и наиболее важным направлением нашей деятельности. Продажи этой продукции составляют примерно 35% от оборота. С середины 2011 г. в нашем ассортименте появились универсальные мобильные батареи, их доля в общем обороте компании достигает 25%. Кстати, данное направление мы планируем усиленно развивать и дальше. На блоки питания для лэптопов приходится 15% сбыта, батареи для фото- и видеокамер — 10%. Оставшиеся 15% разделили между собой защитные пленки для смартфонов, матрицы и клавиатуры для ноутбуков.

PCWeek/UE: Планируете ли вы экспорт продукции или намерены сфокусироваться только на украинском рынке?

А.В.: На данный момент основным рынком сбыта нашей компании является территория Украины. Планов на покорение Европы и ближнего зарубежья пока нет. Но в перспективе расширение бизнеса за счет экспорта мы не исключаем.

PCWeek/UE: С какими крупными корпоративными заказчиками в Украине вы сотрудничаете?

А.В.: Мы сотрудничаем со многими крупными клиентами и партнерами. На сегодня среди постоянных корпоративных клиентов можно отметить: государственное предприятие «Укрзалізниця», аэропорт «Жуляны», а также банки, страховые компании и т. д. В связи с активной деятельностью компании в корпоративном сегменте мы даже приняли решение о формировании соответствующего отдела.

Александр Вовк

Среди наиболее важных партнеров я бы назвал супермаркет электроники «Rozetka», сеть специализированных розничных магазинов по продаже компьютерной техники — «DiaWest — Комп'ютерний світ», интернет-магазин бытовой техники и электроники «АЛЛО» и другие компании.

PCWeek/UE: Какие у вас планы по развитию бизнеса? Есть ли намерения выйти на рынок аккумуляторов для планшетов или запустить в продажу батареи на солнечных элементах?

А.В.: Основной приоритет на 2012 г. — закрепление лидерских позиций. Есть и планы по выводу на рынок новых товарных линеек, однако более конкретно об этом мы расскажем вам позже. А вот рынок аккумуляторов для планшетов на сегодня закрыт: в этих устройствах используются преимущественно встроенные аккумуляторы. Иными словами, пользователь не сможет самостоятельно поменять аккумулятор. Поэтому в случае необходимости рекомендуем воспользоваться УМБ для подзарядки планшета.

Еще несколько лет назад мы протестировали универсальные мобильные батареи на солнечных элементах и пришли к выводу, что такие УМБ не очень эффективны в условиях нашего климата. Ведь в Украине не такой жаркий климат, как, например, в ОАЭ или Египте.

PCWeek/UE: Хотя большинство западных вендоров производят свою продукцию в Китае, название этой страны все еще ассоциируется у большинства украинских потребителей с плохим качеством (часто не без причины). В связи с этим, собираетесь ли вы перенести производство в Украину?

А.В.: Я неоднократно обращал внимание на тот факт, что «Китай Китаю — рознь». Не секрет, что даже такие успешные компании, как Apple, производят продукцию в КНР. Проблема в том, что покупая дешевое ЗУ на рынке, наш соотечественник искренне надеется, что оно будет работать вечно и не испортит технику. Но, к сожалению, некачественная батарея для ноутбуков может стать причиной не только преждевременной смерти устройства, но даже взрыва. Украинский рынок переполнен подделками, поэтому покупатель должен проявлять бдительность.

Вся продукция «Дробак» проходит трехэтапную проверку на заводе на стадии изготовления, а после прибытия товара в Украину — еще одну, финальную. Товары под маркой «Дробак» имеют несколько уровней защиты, начиная от наклейки на товаре и гарантийной пломбы, и заканчивая фирменной упаковкой и логотипом на поверхности. Кроме того, на аккумуляторы для ноутбуков нашего производства мы предоставляем бесплатное гарантийное обслуживание 18 месяцев, хотя многие производители лэптопов на батареи в комплекте дают гарантию не более полугода. Поэтому я не могу согласиться с утверждением, что заводы в Китае выпускают некачественную продукцию.

А вот перенос производства в Украину пока невозможен. К сожалению, сегодня нам рентабельнее привезти продукцию из Китая в Украину, чем провести полный цикл производства в нашей стране. И в ближайшем будущем ситуация вряд ли изменится. Хотя могу однозначно заявить, что мы бы и сами хотели производить нашу продукцию на отечественных предприятиях.

НОВОСТИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

McAfee отмечает значительный прирост числа вредоносов

Компания McAfee опубликовала свой отчет об ИТ-угрозах за 2-й кв. 2012 г., в котором отмечает, что такого прироста количества обнаруживаемых вредоносных программ не наблюдалось уже в течение четырех лет. McAfee Labs обнаружила на 1,5 млн больше вредоносных программ, чем в 1-м кв. 2012 г., и столкнулась с новыми видами угроз безопасности: «попутными загрузками» и программами-вымогателями для мобильных устройств, а также использованием Twitter для управления мобильными бот-сетями. McAfee Labs констатировала быстрое пополнение своего «зоопарка» угроз безопасности образцами вредоносных программ разных видов. Количество вредоносных программ росло со скоростью примерно 100 тыс. образцов в день. В своем отчете McAfee выделила основные разновидности вредоносных программ, представляющих опасность для большого количества пользователей по всему миру.

По заявлению Винсента Уифера (Vincent Weafer), старшего вице-президента McAfee Labs, среди самых крупных атак с использованием вредоносных программ во 2-м кв. 2012 г. можно назвать Flashback, нацеленную на устройства Macintosh, и Flame, объектом которой стал энергетический сектор. После резкого увеличения количества вредоносных программ для мобильных устройств, произошедшего в 1-м кв. 2012 г., темпы распространения вредоносных программ для Android не показывают признаков замедления, вынуждая пользователей находиться в режиме повышенной готовности. Практически все новые вредоносные программы для мобильных устройств, обнаруженные во 2-м кв. 2012 г. (программы для рассылки СМС, мобильные бот-сети, шпионские программы, деструктивные «троянские кони»), были нацелены на платформу Android.

Несмотря на то что вредоносные программы чаще всего поражают персональные компьютеры с программным обеспечением Windows, вредоносную программу можно написать для любой операционной системы и платформы. McAfee предупреждает всех любителей устройств Macintosh о том, что им тоже следует опасаться вредоносных программ, и отмечает стабильный рост темпов распространения вредоносных программ для Macintosh: только в 1-м кв. 2012 г. было обнаружено более 100 новых образцов.

В отчетном кв. снова дали о себе знать бот-сети, продемонстрировав самые высокие за последние 12 месяцев темпы заражения. Крупнейшим в мире местом сосредоточения серверов для управления бот-сетями являются США.

ДАТАЦЕНТРЫ

MiroHost запустил 3D-тур по своему ЦОДу

С 12 сентября на сайте MiroHost.net действует новый для украинских ЦОДов сервис — 3D-тур. Услуга доступна по адресу mirohost.net/#3d-tour и позволяет, не отходя от компьютера, виртуально попасть в датацентр компании, посмотреть изнутри условия обслуживания и оценить качество сервиса ЦОДа. С помощью виртуального тура по всей территории технической площадки реальные и потенциальные клиенты MiroHost могут увидеть, как выглядят серверы в датацентре, какой тип кондиционирования используется, где есть место именно для их сервера и другие важные параметры. Вместе с запуском сервиса 3D-тура, стартует акция от MiroHost — специальный квест по датацентру. Каждый, кто найдет в виртуальном туре значок «MiroHost», получит 80% скидки на покупку любого выбранного им тарифного плана eVPS.

Таким образом максимальная скидка может составить почти 25 тыс. грн для максимального тарифа (eVPS 128) на год, то есть стоимость его составит всего 6240 грн за год. Минимальный же тариф будет стоить всего 130 грн за год.

«Мы хотим показать наш датацентр клиентам, чтобы они видели реальное техническое оснащение и условия эксплуатации оборудования. А это — залог работоспособности их сайтов и сервисов, — подчеркнул директор по маркетингу компании MiroHost Юрий Иванов. — Теперь каждый клиент может оценить наш потенциал технологических мощностей».

При использовании материалов ссылка на сайт pcweek.ua обязательна

РАЗВЕРТЫВАНИЕ ОБЛАЧНЫХ СИСТЕМ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ

КРИС ПРЕЙМСБЕРГЕР

Развертывание облачных систем с открытым исходным кодом началось всего несколько лет назад. Их пока используют в очень немногих производственных системах. Несмотря на то, что ряд предприятий-первопроходцев в области телекоммуникаций, финансовых услуг, науки и СМИ уже вполне освоили альтернативные облачные системы с открытым исходным кодом, о них знают лишь немногие малые и средние компании. Чтобы представить нашим читателям сбалансированный взгляд на эту проблему, редакция подготовила материал на основе информации, полученной от Флойда Стримлинга, ярого сторонника компьютерных решений из техасской компании Zenoss.

ПЯТЬ ДОВОДОВ «ЗА»

1. Гибкость

По определению облака с открытым исходным кодом обеспечивают более высокую гибкость, чем их патентованные конкуренты. Вместо изучения руководств и посещения практических занятий клиенты могут читать и модифицировать сам код и участвовать в различных проектах. Взаимодействие с разработчиками и заимствование их опыта обеспечивают клиентам дополнительную гибкость при проектировании облака и инновационные решения для внутреннего или более широкого использования.

2. Отсутствие привязки к определенному производителю

Один из боевых кличей сторонников облаков с открытым исходным кодом — «Никакой привязки к производителям!». Идея довольно проста: если вы создаете облако на основе открытой и широко распространенной технологии с открытым исходным кодом, никакой производитель не властен над вашей инфраструктурой. Кроме того, облака с открытым исходным кодом обеспечивают клиентам свободу выбора создаваемого облака в соответствии со своими потребностями и целями бизнеса вместо замкнутости в рамках одного патентованного решения.

3. Экономия

Открытое ПО обладает существенными ценовыми преимуществами перед патентованным. Действительно, когда клиенты решают использовать полностью открытое или коммерческое открытое ПО, они могут существенно экономить. А возможность снизить затраты и одновременно повысить свою гибкость дает огромное преимущество любой организации.

4. Управление, открытые стандарты и API-интерфейсы

В облаке с открытым исходным кодом используют открытые стандарты и API-интерфейсы, которые не являются собственностью какого-либо производителя. Это позволяет клиентам распоряжаться аппаратной инфраструктурой и управляющей платформой облака независимо от используемой технологии. Кроме того, открытые API-интерфейсы обеспечивают интеграцию с имеющимися открытыми или патентованными решениями.Благодаря этому вложенные вами в ИТ средства не обесценятся при переходе на новую архитектуру.

5. Переносимость

При создании облака с открытым исходным кодом следует посмотреть, как оно интегрируется с публичными, частными и гибридными облаками. Выбор открытой технологии увеличивает количество вариантов в рамках более широкой облачной экосистемы. Клиенты могут не ограничивать выбор совместимостью с патентованной технологией, а поискать другие облачные технологии с открытым исходным кодом, которые сочетаются с используемыми ИТ, их потребностями и целями бизнеса.

ПЯТЬ ДОВОДОВ «ПРОТИВ»

1. Якобы слабая техническая поддержка

Клиенты, решившие создавать облака с открытым исходным кодом на полностью открытом ПО, попадут в зависимость от соответствующих проектов в плане технической поддержки. Поддержка будет оказываться в форме краудсорсинга — через форумы, чаты IRC, перечни вопросов и ответов или журналирование дефектов в системах выявления ошибок. С другой стороны, клиенты могут выбрать для создания облаков коммерческое открытое ПО. В этом случае слабости технической поддержки будут не столь ощутимы.

2. Привязка к определенному производителю

Некоторые пользователи предпочитают комфорт и безопасность, полагаясь на решение одного производителя, а также его услуги в вопросах технической поддержки, тестирования и интеграции системы. Если клиенты, работающие с одним патентованным решением, расширяют свой выбор, они могут запутаться. Это приведет к замедлению стратегических проектов из-за отсутствия необходимого опыта.

3. Затраты

Облака с открытым исходным кодом действительно дают существенную экономию на лицензионных отчислениях по сравнению с конкурирующими патентованными решениями. Но есть и другие затраты, которые невозможно игнорировать. Для обслуживания инфраструктуры облаков с открытым исходным кодом могут потребоваться штатные опытные разработчики и администраторы,а также консультанты или программисты со стороны.

4. Незрелость технологий

Поскольку экосистема облаков с открытым исходным кодом продолжает развиваться, клиенты могут усомниться в зрелости проектов с открытым исходным кодом. При создании открытого облака выбор технологии, сделанный менеджером сегодня, в будущем может стать преследующим его кошмаром. В условиях конкуренции различных проектов с открытым исходным кодом и при наличии множества вариантов выбора клиенту иногда трудно разобраться, в каком направлении следует двигаться.

5. Оно того стоит?

Пользователи хотят, чтобы облачная инфраструктура обладала высокой доступностью, была простой в использовании и достаточно подвижной для развития наряду с бизнесом. Прежде чем создавать облачную инфраструктуру, необходимо проанализировать цели бизнеса и рационализировать используемую ИТ-инфраструктуру. В конечном счете может оказаться, что вам не следует создавать свое облако, а стоит присмотреться к альтернативным решениям, включая аутсорсинг и услуги типа «инфраструктура как сервис»(IaaS) или «платформа как сервис»(PaaS).

ПОТРАТИВ ВСЕГО 5 МИНУТ НА ЗАПОЛНЕНИЕ АНКЕТЫ, ВЫ БУДЕТЕ БЕСПЛАТНО ПОЛУЧАТЬ PC Week/UE В ТЕЧЕНИЕ 6 МЕСЯЦЕВ

PC WEEK UKRAINIAN EDITION

Уважаемые читатели!

Только полностью заполненная анкета, рассчитанная на руководителей, отвечающих за автоматизацию предприятий; специалистов по аппаратному и программному обеспечению, телекоммуникациям, сетевым и информационным технологиям из организаций, имеющих более **50 компьютеров**, дает **право на бесплатную подписку** на газету PC Week/UE в течение полугода с момента получения анкеты. Пожалуйста, будьте внимательны при заполнении анкеты!

Примечание. На домашний адрес PC Week/UE по бесплатной корпоративной подписке не высылается. Данная форма подписки распространяется на территорию Украины.

Вы можете получить анкету в электронном виде, пишите на адрес: anketa@skukraine.com

Название организации: _____

Почтовый адрес организации: _____

Индекс: _____ Область: _____

Город: _____

Улица: _____ Дом _____

Фамилия, имя, отчество: _____

Подразделение/отдел: _____

Должность: _____

Телефон: _____ Факс: _____

E-mail: _____ WWW: _____

Правила заполнения анкеты:
1. Записать полные данные по Вашему предприятию.
2. Поставить «✓» напротив выбранной Вами информации

1. К какой отрасли относится Ваше предприятие?

1. Энергетика ☐
2. Связь и телекоммуникации
3. Производство, не связанное с вычислительной техникой (добывающие и перерабатывающие отрасли, тяжелая индустрия, машиностроение и т.п.) ☐
4. Финансовый сектор (кроме банков) ☐
5. Банковский сектор ☐
6. Архитектура и строительство ☐
7. Торговля товарами, не связанными с информационными технологиями
8. Транспорт
9. Информационные технологии (см. также вопрос 2) ☐
10. Реклама и маркетинг ☐
11. Научно-издательская деятельность (НИИ и вузы) ☐
12. Государственно-административные структуры ☐
13. Военные организации ☐
14. Образование ☐
15. Медицина ☐
16. Издательская деятельность и полиграфия ☐
17. Иное (что именно) _____

2. Если основной профиль Вашего предприятия - информационные технологии, то уточните, пожалуйста, сегмент, в котором предприятие работает:

1. Системная интеграция ☐
2. Дистрибуция ☐
3. Телекоммуникации ☐
4. Сборка и производство аппаратного обеспечения ☐
5. Продажа компьютеров ☐
6. Ремонт компьютерного оборудования ☐
7. Разработка и продажа ПО ☐
8. Консалтинг ☐
9. Иное (что именно) _____

3. Форма собственности Вашей организации (только один пункт)

1. Госпредприятие ☐
2. ОАО (открытое акционерное общество) ☐
3. ЗАО (закрытое акционерное общество) ☐
4. Зарубежная фирма ☐
5. СП (совместное предприятие) ☐
6. ЧП (частное предприятие) ☐
7. Иное (что именно) _____

4. К какой категории относится подразделение, в котором Вы работаете? (только один пункт)

1. Дирекция ☐
2. Информационно-аналитический отдел ☐
3. Техническая поддержка ☐
4. Служба АСУ/ИТ ☐
5. ВЦ ☐
6. Инженерно-конструкторский отдел (САПР) ☐
7. Отдел рекламы и маркетинга ☐
8. Бухгалтерия/Финансы ☐
9. Производственное подразделение ☐
10. Научно-исследовательское подразделение ☐
11. Учебное подразделение ☐
12. Отдел продаж ☐
13. Отдел закупок/логистики ☐
14. Иное (что именно) _____

5. Ваш должностной статус (только один пункт)

1. Директор/президент/владелец ☐
2. Зам. директора/вице-президент ☐
3. Руководитель подразделения ☐
4. Сотрудник/менеджер ☐
5. Консультант ☐
6. Иное (что именно) _____

6. Ваш возраст

1. До 20 лет ☐
2. 21-25 лет ☐
3. 26-30 лет ☐
4. 31-35 лет ☐
5. 36-40 лет ☐
6. 41-50 лет ☐
7. 51-60 лет ☐
8. Более 60 лет ☐

7. Численность сотрудников в Вашей организации

1. Менее 10 человек ☐
2. 10-100 человек ☐
3. 101-500 человек ☐
4. 501-1000 человек ☐
5. 1001-5000 человек ☐
6. Более 5000 человек ☐

8. Численность компьютерного парка Вашей организации

1. 10-20 компьютеров ☐
2. 21-50 компьютеров ☐
3. 51-100 компьютеров ☐
4. 101-500 компьютеров ☐
5. 501-1000 компьютеров ☐
6. 1001-3000 компьютеров ☐
7. 3001-5000 компьютеров ☐
8. Более 5000 компьютеров ☐

9. Какие ОС используются в Вашей организации?

1. Windows 9x/ME/2K/XP/Vista ☐
2. Windows Server 2K/2003/2008/Small Business/Essential Business ☐
3. OS/2 ☐
4. MacOS ☐
5. AIX ☐
6. Solaris/SunOS ☐
7. OS/400 ☐
8. HP/UX ☐
9. Novell ☐
10. FreeBSD ☐
11. Linux (какой именно дистрибутив) ☐
12. Другие UNIX-подобные ОС (какие именно) ☐
13. Иное (что именно) _____

10. Коммуникационные возможности компьютеров Вашей организации

1. Объединены в ЛВС ☐
2. Имеют распределенные ресурсы ☐
3. Имеют выход в Интернет (каким способом) ☐
4. Объединены с ЛВС в других филиалах/офисах ☐
5. Организована мультисервисная сеть (аудио/видео/данные) ☐
6. Не объеденины между собой ☐

11. Сетевое оборудование каких производителей используется в Вашей организации?

1. Alcatel-Lucent ☐
2. Allied Telesis ☐
3. ASUS ☐
4. Avaya ☐
5. Cisco Systems ☐
6. D-Link ☐
7. Ericsson ☐
8. Huawei ☐
9. Edimax ☐
10. Enterasys ☐
11. Linksys ☐
12. NetGear ☐
13. Nortel ☐
14. ProCurve (HP) ☐
15. TrendNet ☐
16. ZyXEL ☐
17. Другое (что именно) _____ ☐
18. Не установлено никакое ☐

12. Имеет ли сеть Вашей организации территориально распределенную структуру (охватывает более одного здания)?

1. Да ☐ 2. Нет ☐

13. Собирается ли Ваше предприятие устанавливать мультисервисную сеть в ближайший год?

1. Да ☐ 2. Нет ☐

14. Сколько серверов в сети Вашей организации?

_____

15. Если в Вашей организации используются серверы класса Enterprise, то на базе какой архитектуры?

1. RISC-архитектура (какие именно процессоры) ☐
2. Itanium-архитектура (какие именно процессоры) ☐
3. x86-архитектура (какие именно процессоры) ☐
4. Иное (что именно) _____
5. Не используются ☐

16. Компьютеры каких фирм-изготовителей используются на Вашем предприятии?

	Настольные ПК	Портативные ПК	Серверы
Asus	☐	☐	☐
Dell	☐	☐	☐
Fujitsu	☐	☐	☐
Hewlett-Packard	☐	☐	☐
IBM	☐	☐	☐
Lenovo	☐	☐	☐
Oracle/Sun	☐	☐	☐
Samsung	☐	☐	☐
Sony	☐	☐	☐
Toshiba	☐	☐	☐

Иное (что именно) _____

17. Какое прикладное ПО используется в Вашей организации?

1. Средства разработки ПО ☐
2. Офисные приложения ☐
3. СУБД ☐
4. Бухгалтерские и складские программы ☐
5. Издательские системы ☐
6. Графические системы ☐
7. Статистические пакеты ☐
8. ПО для управления производственными процессами ☐
9. Клиенты электронной почты ☐
10. САПР ☐
11. Браузеры Internet ☐
12. Web-серверы ☐
13. Системы управления ресурсами предприятия (ERP-системы) ☐
14. Системы управления отношениями с клиентами (CRM-системы) ☐
15. Системы бизнес-аналитики (BI-системы) ☐
16. Иное (что именно) _____

18. Если в Вашей организации используются бизнес-приложения (ERP-, CRM-, BI-системы и ПО для автоматизации бюджетирования), то каких фирм-разработчиков?

1. 1C ☐
2. Галактика ☐
3. Парус ☐
4. HansaWorld ☐
5. IBM (Cognos) ☐
6. Microsoft ☐
7. Naumen ☐
8. Novell ☐
9. Oracle ☐
10. SAP ☐
11. Terrasoft ☐
12. Другое (что именно) _____ ☐
13. Не установлено никакое ☐

19. Если в Вашей организации используются ПО для обеспечения безопасности, то каких фирм-разработчиков?

1. Доктор Веб ☐
2. Лаборатория Касперского ☐
3. CA (Computer Associates) ☐
4. Check Point ☐
5. Cisco Systems ☐
6. McAfee ☐
7. Novell ☐
8. Symantec ☐
9. Trend Micro ☐
10. Другое (что именно) _____ ☐
11. Не установлено никакое ☐

20. Существует ли на Вашем предприятии единая корпоративная информационная система?

1. Да ☐ 2. Нет ☐

21. Если Ваша организация не имеет своего Web-узла, то собирается ли она в ближайший год его завести?

1. Да ☐ 2. Нет ☐

22. Если Вы используете СУБД в своей деятельности, то какие именно?

1. Adabas ☐
2. Cache ☐
3. DB2 ☐
4. dBase ☐
5. FoxPro ☐
6. Informix ☐
7. Ingress ☐
8. MS Access ☐
9. MS SQL Server ☐
10. MySQL ☐
11. Oracle ☐
12. Postgress ☐
13. Sybase ☐
14. Не используем ☐
15. Иное (что именно): ☐

23. Как Вы оцениваете свое влияние на решение о покупке средств информационных технологий для своей организации? (отметьте один пункт)

1. Принимаю решение о покупке (подписываю документ) ☐
2. Составляю спецификацию (выбираю средства) и рекомендую приобрести ☐
3. Не участвую в этом процессе ☐
4. Иное (что именно) _____

24. На приобретение каких из перечисленных групп продуктов или услуг Вы оказываете влияние (покупаете, рекомендуете, составляете спецификацию)?

Системы
1. Серверы ☐
2. Рабочие станции ☐
3. ПК/автоматизированные рабочие места ☐
4. Тонкие клиенты/сетевые компьютеры ☐
5. Ноутбуки ☐
6. Планшеты ☐

Сети
7. Активное сетевое оборудование ☐
8. Пассивное сетевое оборудование ☐
9. Компоненты беспроводных сетей ☐
10. Компоненты глобальных сетей ☐

Периферийное оборудование
11. Принтеры/МФУ ☐
12. Мониторы ☐
13. ИБП (UPS) ☐

Память
14. Различные накопители ☐
15. Системы архивирования ☐
16. SAN-компоненты ☐

Программное обеспечение
17. Электронная почта ☐
18. СУБД ☐
19. Сетевое ПО ☐
20. Электронная коммерция ☐
21. ПО для Web-дизайна ☐
22. ПО для Интернета ☐
23. Java ПО ☐
24. Операционные системы ☐
25. Мультимедийные приложения ☐
26. Средства разработки программ ☐
27. CASE-системы ☐
28. САПР (CAD/CAM) ☐
29. Системы управления проектами ☐
30. ПО для архивирования ☐
31. Бизнес-приложения (ERP-, CRM-, BI-системы) ☐

Внешние сервисы
32. ☐

Ничего из вышеперечисленного
33. ☐

25. Каков наивысший уровень, для которого Вы оказываете влияние на покупку компьютерных изделий или услуг (служб)?

1. Более чем для одной компании ☐
2. Для всего предприятия ☐
3. Для подразделения, располагающегося в нескольких местах ☐
4. Для нескольких подразделений в одном здании ☐
5. Для одного подразделения ☐
6. Для рабочей группы ☐
7. Только для себя ☐
8. Не влияю ☐
9. Иное (что именно) _____

26. Через каких провайдеров в настоящее время Ваша фирма получает доступ в Интернет и другие Интернет-услуги?

1. Укртелеком ☐
2. Астелит (Life) ☐
3. Datagroup ☐
4. Киевстар/Beeline ☐
5. MTS ☐
6. Vega ☐
7. Lucky Net ☐
8. Intellecom ☐
9. UNTC ☐
10. Украинская Мультисервисная Сеть (ТелеХаус) ☐
11. Релком ☐
12. Українські новітні технології (Freshtel) ☐
13. PEOPLEnet ☐
14. ColoCall ☐
15. Mirolink.net ☐
16. Воля ☐
17. Через других (каких именно): ☐

_____

27. Из каких источников Вы узнали о газете?

_____

_____

_____

_____

Дата заполнения_____

Заполненную анкету пришлите по адресу:

01135, г. Киев, просп. Победы 5, офис 9

При использовании материалов ссылка на сайт pcweek.ua обязательна

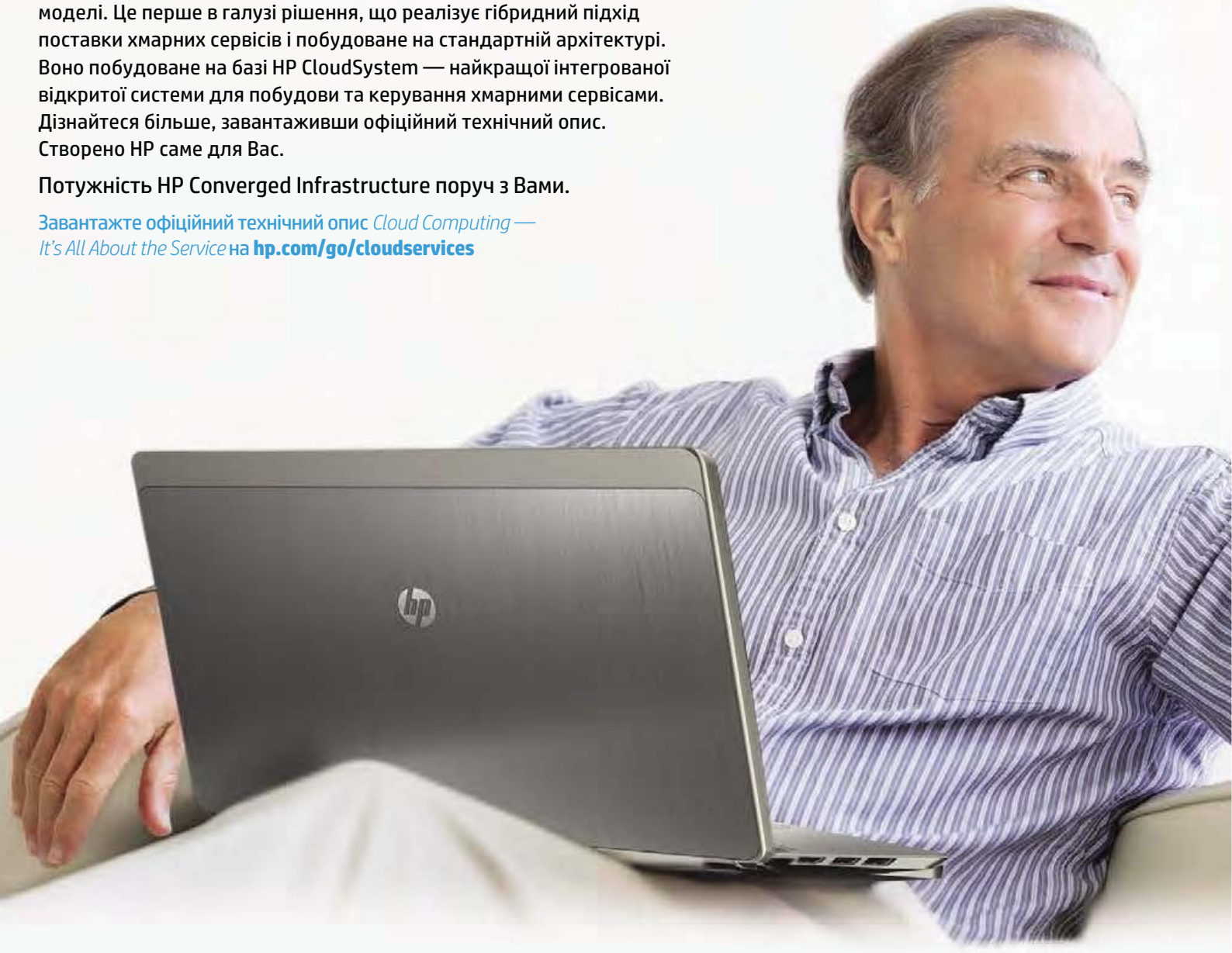
У чому, на Вашу думку, суть «Cloud Master»?

Розкрийте для себе силу та потужність технології Cloud Computing (хмарних обчислень) в будь-якій точці середовища разом з HP.

Створюйте та керуйте сервісами в хмарному середовищі за допомогою **HP Converged Cloud** — професійного рішення, що дозволяє використовувати приватну, публічну та гібридну моделі. Це перше в галузі рішення, що реалізує гібридний підхід поставки хмарних сервісів і побудоване на стандартній архітектурі. Воно побудоване на базі HP CloudSystem — найкращої інтегрованої відкритої системи для побудови та керування хмарними сервісами. Дізнайтеся більше, завантаживши офіційний технічний опис. Створено HP саме для Вас.

Потужність HP Converged Infrastructure поруч з Вами.

Завантажте офіційний технічний опис *Cloud Computing — It's All About the Service* на **hp.com/go/cloudservices**



© Copyright 2012 Hewlett-Packard Development Company, L.P. Наведена у цьому документі інформація може змінюватися без попереднього повідомлення. HP надає лише ті гарантії на свої продукти на послуги, які викладені у гарантійних зобов'язаннях, що додаються до цих продуктів та послуг. Ніякі відомості у даному документі не можуть розглядатися як додаткові гарантійні зобов'язання. HP не несе відповідальності за технічні, редакторські та інші помилки у даному документі.

Клауд Мастер, Клауд Комп'ютінг, ЕйчПі Конверджд Клауд, ЕйчПі Клауд Систем, ЕйчПі Конферджд Інфрастракче, Клауд Комп'ютінг — Ітс Ол Ебаут Зе Сервіс, Х'юлетт-Паккард Девелопмент Компані, Ел.Пі.