



КАКОЙ УРОВЕНЬ БЕЗОПАСНОСТИ НЕ БУДЕТ МЕШАТЬ РАЗВИТИЮ ИНТРАНЕТА?

Алексей Лукацкий

Бизнес-консультант по безопасности

Содержание

- **Определимся с терминами**
- **Архитектура защиты**
- **Истинная проблема**
- **Как решать?**
- **Примеры из жизни**



ОПРЕДЕЛИМСЯ С ТЕРМИНАМИ



Зачем нужна Интранет?

Любая корпорация представляет из себя сумму компетенций...

- **Находящихся или в головах сотрудников**
- **Или существующих в виде правил, инструкций, техзаданий, баз данных, оперативной информации, культуры компании**

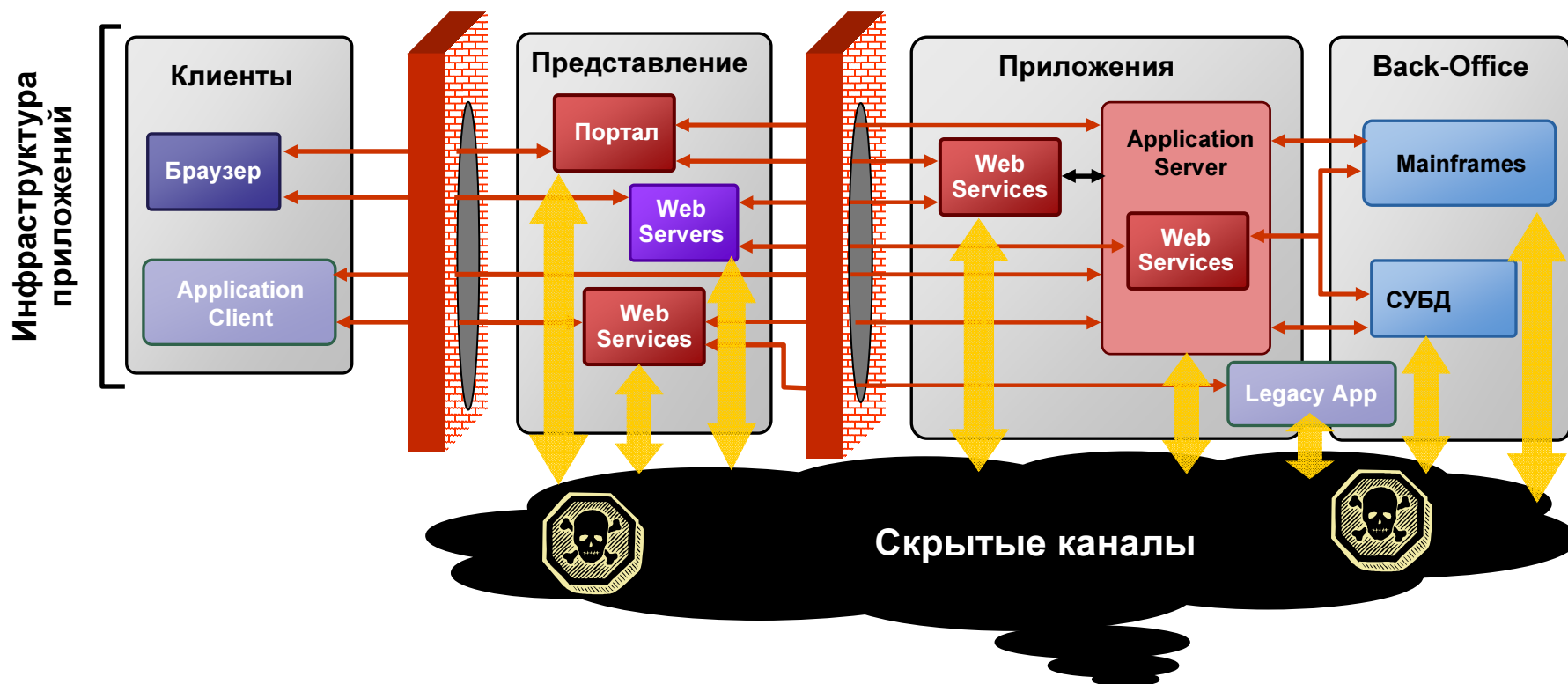
Каким образом сделать их доступными для каждого сотрудника, избежав неизбежной информационной перегрузки...

- **Найти нужных людей с нужными знаниями и навыкам**
- **Оперативно найти правильную и нужную информацию**
- **Обучить сотрудников**
- **Организовать их работу**

АРХИТЕКТУРА ЗАЩИТЫ



Классическая схема защиты

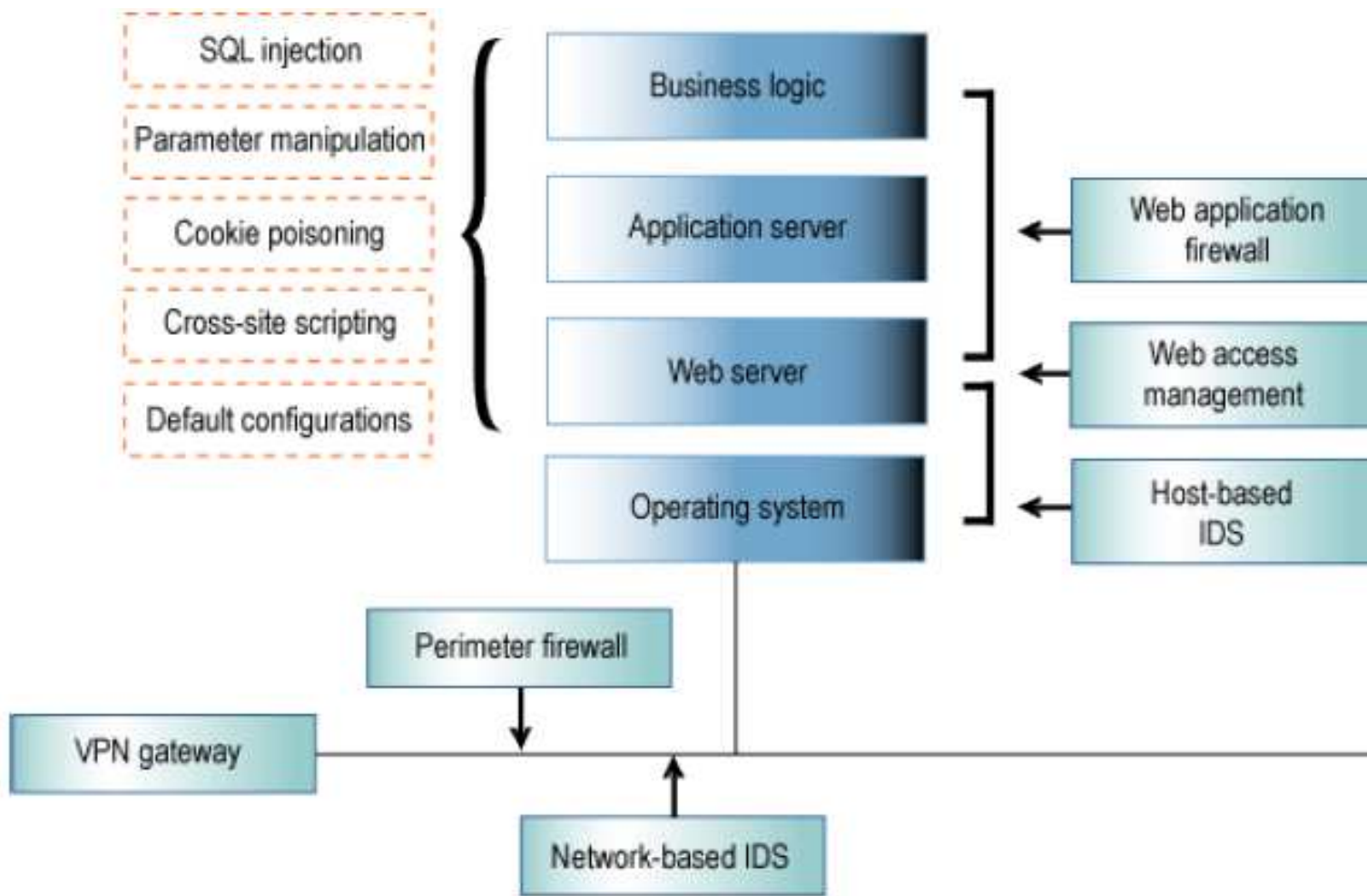


- Классическая схема защиты периметра не способна обезопасить Интранет от направленных угроз...

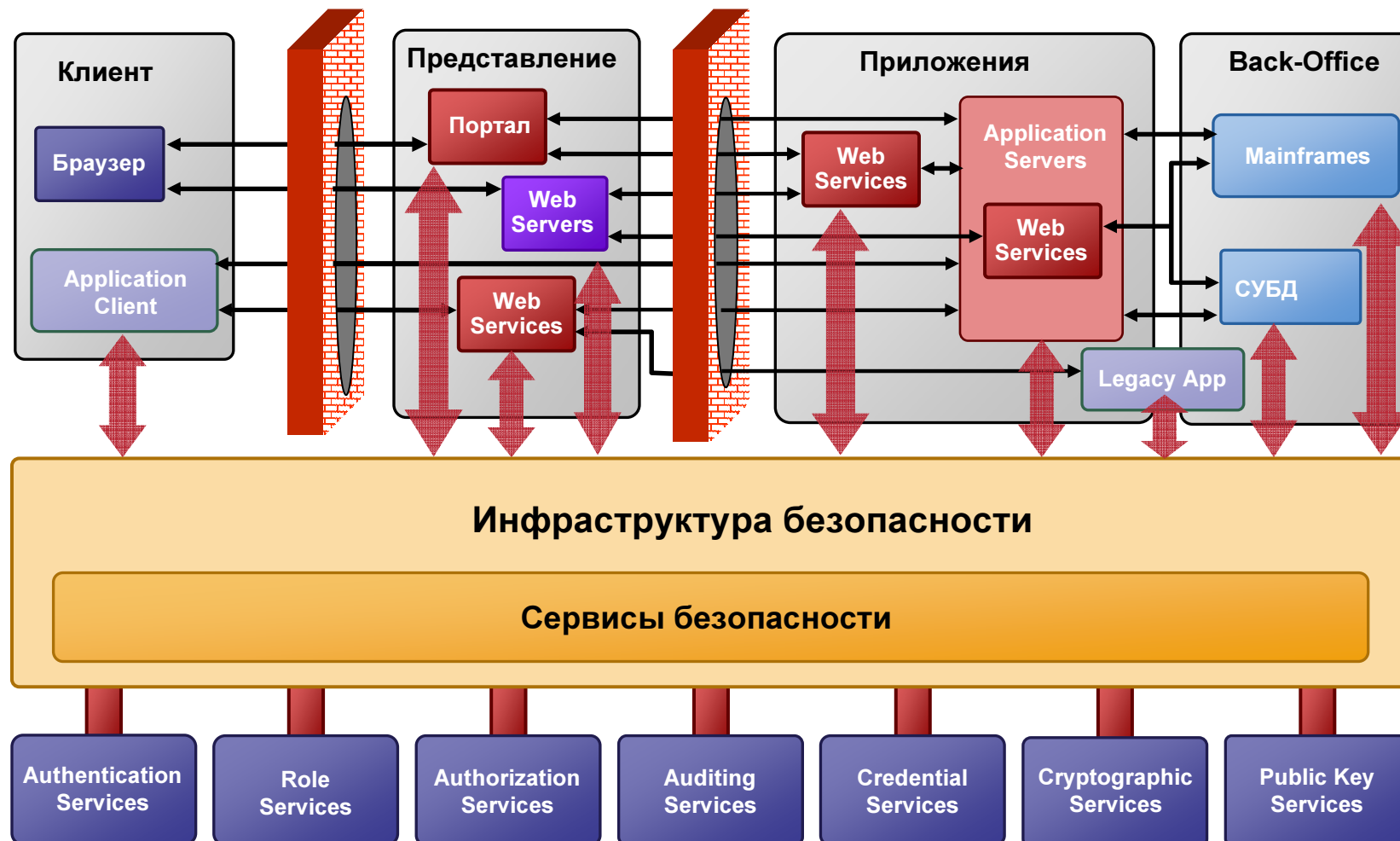
Модель угроз

Угроза	Атака / уязвимость	Последствия	Меры первой помощи
Внешние нарушители <ul style="list-style-type: none"> • Хакеры • Преступники • Другие 	Denial of service Раскрытие/утечка Модификация Атака Шалости в системе	Продуктивность Финансы Репутация Взаимодействие	Шифрование Web-сервисов Защита периметра Зонирование
Внутренняя угроза <ul style="list-style-type: none"> • Привилег. пользователь • Админ 	Закладка Раскрытие/утечка Модификация Атака Шалости в системе	Финансы Репутация Взаимодействие	Управление Identity Сдерживание Персонал, аудит, юридические меры

Архитектура защиты



Сервис-ориентированная схема защиты



“Защита Интранет – это обеспечение авторизованного доступа легитимным субъектам в нужное время на требуемый период времени с требуемым качеством.”

ИСТИННАЯ ПРОБЛЕМА



Инtranет Cisco Systems

- **Внешний портал**

Корпоративная информация

Продукты

Продажи

Вакансии

Партнеры...

- **Внутренний портал**

Самообслуживание
сотрудников

Проповедник культуры

- **Производственный портал**

ERP

SCM...

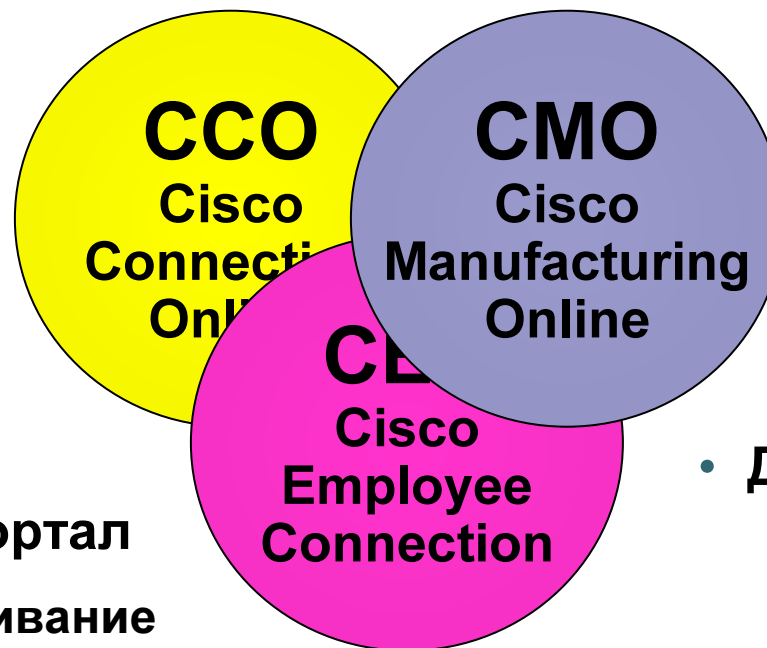
- **Другие порталы**

PEC

Management

Finance

Security...



Инtranет Cisco: “Как я делаю мою работу”

Управление ресурсами

- Facilities Service Request Facilities Move Request
- Package Tracking (RIPIT)
- Incident/Hazard report
- Maps & Floorplans
- Building Locations & Head
- DPC Job Submission
- MeetingPlace
- Catering Request
- Corporate Events Calendar
- Meeting & Events Support
- Metro
- Travel Profile
- Ariba
- EBC Meeting Request
- Ridesharing

Коммуникации и

- Mailer
- HR Mailing Lists
- FogFind
- News/Announcements
- News Posting
- Send a Page
- Banner Generator
- StarViper
- Product Manager Locator
- Video Conferencing
- WebCast
- Company Meeting Live and Rebroadcast

Внутреннее ИТ обслуживание

- Support Finder
- TRC
- ECS
- Sales

Услуги для сотрудников

- Employee Referral Program
- HR Address Change
- Friends Campaign
- Events Registration

Миллионы страниц
Гигабайты данных
Сотни приложений
Глобальный доступ 40000+ сотрудников
Всего 42,000,000+ обращений в месяц
1000 обращений в
среднем в месяц каждым сотрудником
50 страниц просматривается
за один день

alendar
ard Reporting
t Request
nin

mpensation)

Submission
l Requisitions

сы и рыночная мация

Tracker (Budget vs Actual)

ve Financial Analysis
& Documentation Order

als
ions

Order Inquiry

- Order Status Reporting
- Sales Webreports
- Financial Data Directory

- BSG video on Demand
- TAC Training video
- Manufacturing Training
- Cisco Interactive Mentor

Инtranет Chevron

- **Число сотрудников**

 - В штате – 50,000

 - Контрактников – 20,000

 - Других – 7,000

- **Типы идентификаторов**

 - Пользовательские (Windows, Linux...)

 - Административные

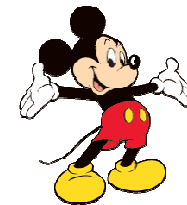
 - К устройствам (ПК, КПК...)

 - К приложениям (SAP, Oracle...)



Инtranет Disney

- **Число сотрудников – 120,000**
Из них 60,000 в одном офисе
- **Сотни приложений**
Собственноручно разработанные и приобретенные
- **ПК и КПК**



The **WALT DISNEY** Company

Инtranет GM

- **Люди**

400,000 пользователей с логическим доступом к системам GM: сотрудники, контрактники, поставщики, дилеры, продавцы, дистрибуторы, альянс-партнеры

Свыше 1 миллиона пользователей, включая бывших служащих и покупателей

- **Технологии и приложения**

400+ серверов Active Directory и 100+ серверов Sun LDAP

6 главных порталов и свыше 100 малых порталов

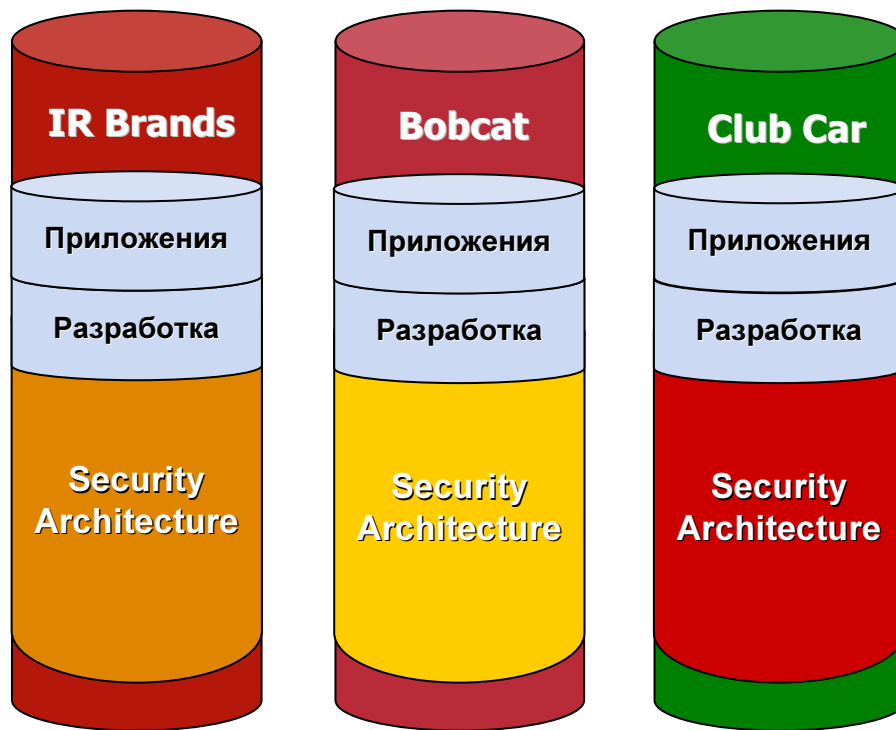
3000 приложений

- **От 12 до 40 (!) ID и паролей на каждого**



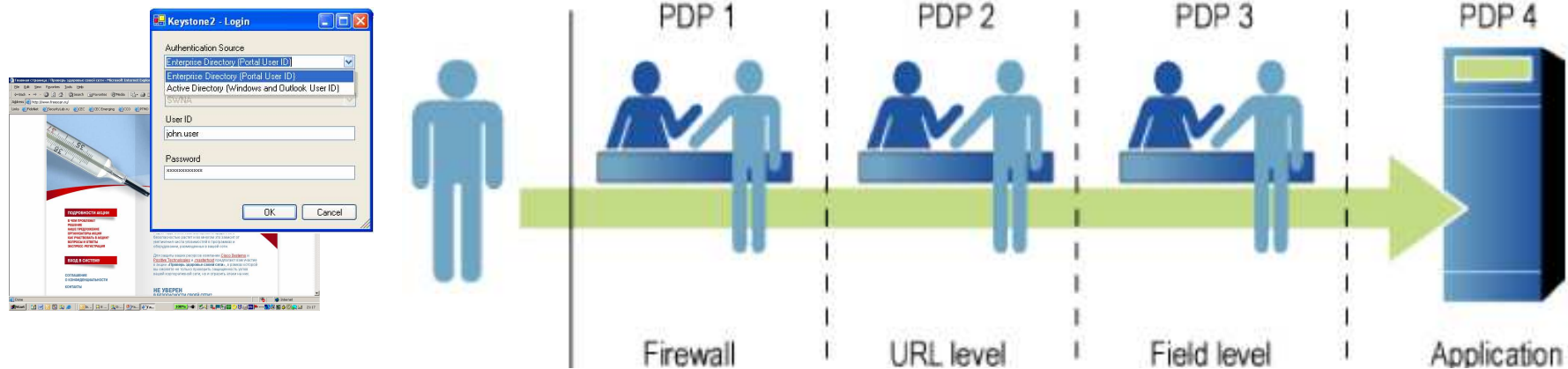
Инtranет Ingersoll Rand

Технологические порталы



- IR растет за счет слияний и поглощений
- Каждый бренд имеет свои порталы
- Дублирование затрат по всей IR
- Пользователи теряют время

Identity Management - за сценой



- **Пользователь вводит имя/пароль и все...
остальное остается за пределами его внимания**
- **Процесс аутентификации, авторизации является самым сложным в порталъных (интранет) технологиях**

Аутентификация – в чем проблема?



Пример расчета

- **Число пользователей – 120000**
- **Ежегодная ротация кадров – 15%**
- **Среднее число ID/паролей – 5**
- **Число рабочих часов в день – 8**
- **Число рабочих дней в год - 220**

Первая фаза расчета – установка ID

- Ежегодное число новых пользователей – 18000 (120000*15%)
- Необходимо поддерживать 90000 новых ID/паролей (5*18000)
- Создание нового ID/пароля – в среднем 120 секунд (анализ заявки, создание и настройка учетной записи)
- Всего на администрирование новых пользователей уходит **3000 часов (~2 человека при полной нагрузке)**

Вторая фаза расчета – ежедневная работа

- В среднем **20** входов в систему/приложения ежедневно (из-за истекшего таймаута, смены приложения и т.д.)
- Среднее время регистрации – **15** секунд
- Ежедневно тратится **10000** ресурсо-часов на регистрацию
- Ежегодно тратится **2200000** ресурсо-часов на регистрацию в разные системы и приложения

Третья фаза расчета – проблемы

- В среднем **1%** всех попыток регистрации заканчивается неудачно
- Повторная регистрация разрешается через **60 секунд**
- Общее время на повторную регистрацию в год составляет **88000 часов**

Четвертая фаза расчета – поддержка

- В среднем после 3-х неудачных попыток входа в систему учетная запись блокируется
- После 2-х неудачных попыток входа рекомендуется позвонить в службу поддержки
- 2400 звонков ежедневно в службу поддержки по факту 2-х неудачных попыток входа в систему
- SLA = 4 часа на обработку одного инцидента
- 18000 пользователей ждут максимум по 4 часа – 72000 часа потери времени (продуктивности)
- 2400 звонка максимум по 4 часа – 9600 часов в день или **2112000 ресурсо-часов** в год

Итого

- **Время затраченное на администрирование новых ID/паролей, ежедневную регистрацию и повторные ввод ID/пароля составляет 2291000 часов в год...**

что составляет 1% всего рабочего времени компании

- **Еще 2184000 ресурсо-часов в год на поддержку неудачных попыток входа...**

что также больше 1% всего рабочего времени компании

- **Итого – 4475000 ресурсо-часов или больше 2% всего рабочего времени компании в год - только на одну задачу – управление Identity**

General Motors - факты

- Предоставление доступа в среднем через 7 дней
- Синхронизация паролей и ID – 3 дня
- 50% запросов требует контактов с пользователем
- «Разруливание» проблем с доступом – 10 дней
- Конфликт между ID может приводить к задержкам в работе до 90 дней

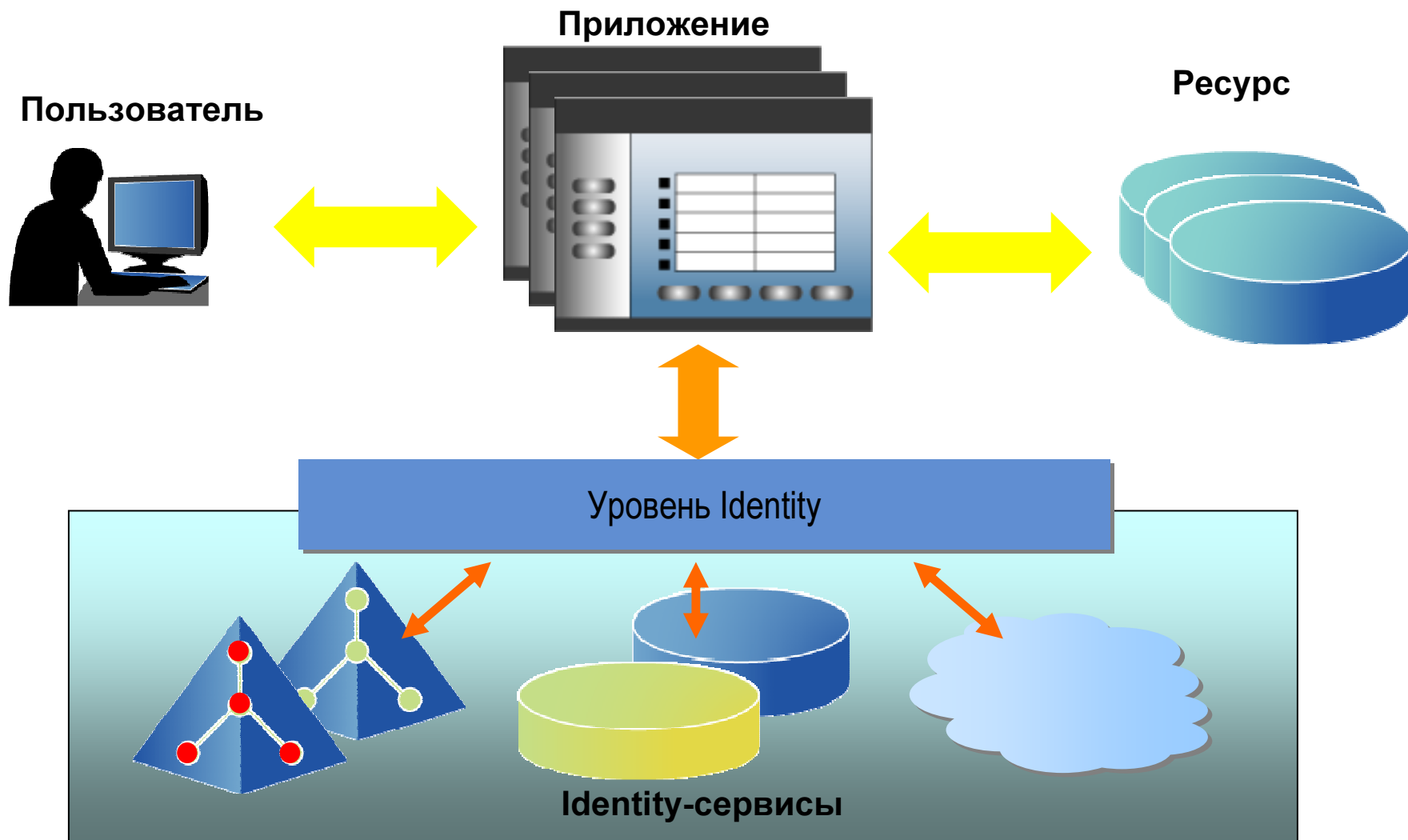
General Motors - потери

- **Обработка 6600 проблем с доступом – потеря продуктивности – 3,000,000 долларов**
- **Восстановление доступа для 56000 профилей – потеря продуктивности – 18,200,000 долларов**
- **2500 профилей не требуют доступа – затраты на удаление – 162,500 долларов**
- **Прямой ущерб – 1,200,000 долларов**

КАК РЕШАТЬ



Как правильно решить задачу



Стандарты защиты Web-сервисов

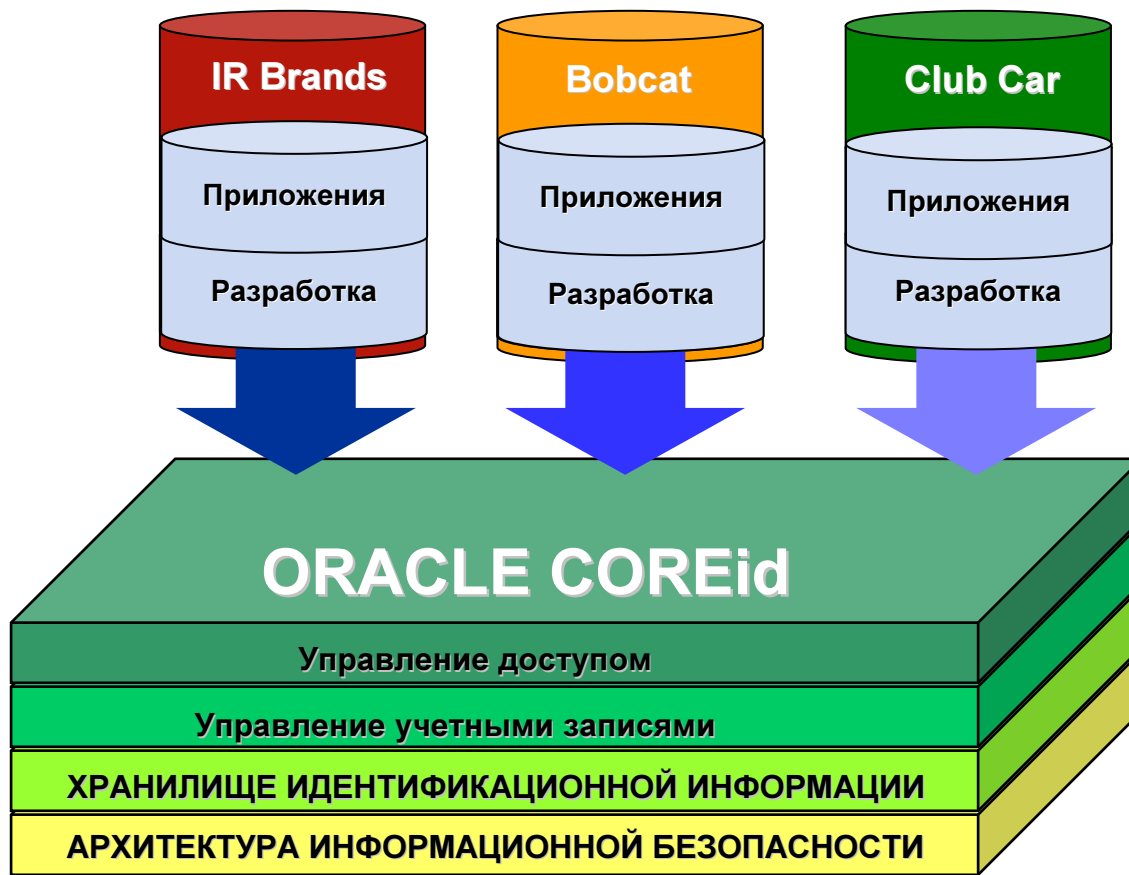
- **SAML**
- **XACML**
- **SPML**
- **WS-Security**
- **SASL**
- **И Т.Д.**

Примеры решений

- **Obliv**
- **Netegrity**
- **IBM**
- **Novell**
- **Oracle**
- **Entrust**
- **SUN**
- **RSA**

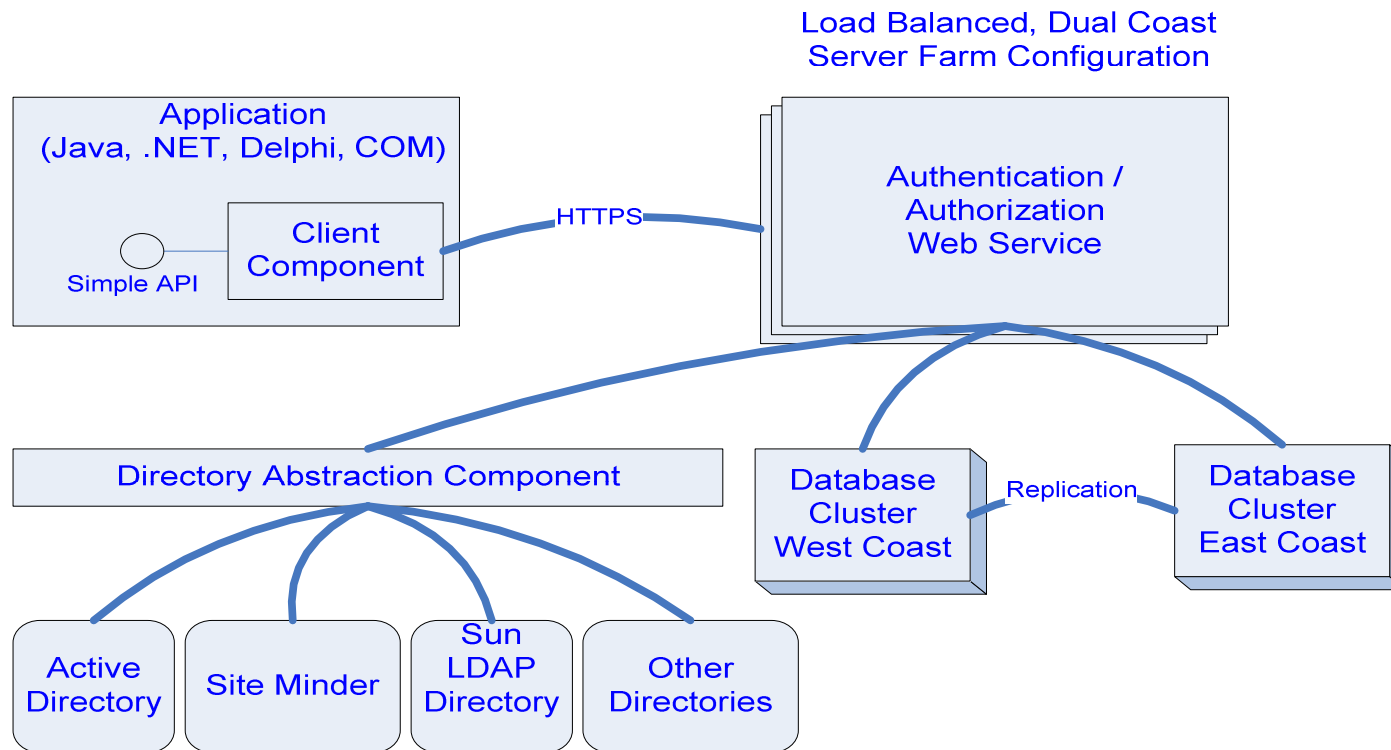
Ingersoll Rand выбрал Oracle

Unified Identity Management



- IR с «одним лицом»
- Единый интерфейс управления
- Экономия при масштабировании
- Устранение точечных решений
- Single Sign-on

Disney Keystone своими руками



ЭФФЕКТ ОТ ВНЕДРЕНИЯ



Примеры реализации

- **GM**

Время обеспечения доступа снизилось с 7 дней до 7 минут

Все учетные записи были заменены на одну

- **BMW**

Средняя частота использования User Self Service до внедрения ASPR: < 50% (до 2004 < 30%)

Средняя частота использования User Self Service после внедрения ASPR: ~ 92%

ROI – 6 месяцев



Примеры реализации

- **Charles Schwab**

 - Доступность – 99.95%

 - Изменения в back end не влияют на пользователей

 - Плохие бизнес-процессы стали видны «лучше»

- **Chevron**

 - Интеграция с картой доступа в помещения

 - Биометрическая аутентификация в ключевые сервисы

ЗАКЛЮЧЕНИЕ

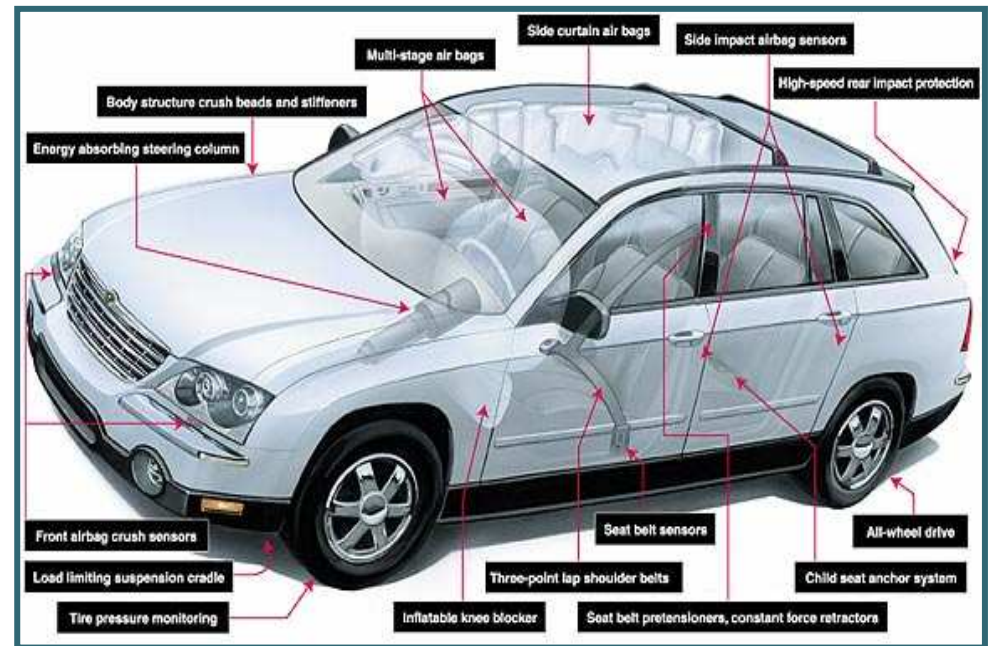


Компромисс удобства и безопасности



Безопасность, как опция

- Рост сложности
- Высокая стоимость интеграции
- Медленное внедрение
- Сложность администрирования
- Нет сквозной функциональности
- Отражение не всех угроз
- Низкая надежность



Безопасность, как часть системы

- Снижение сложности
- Тесная интеграция сетевых сервисов и приложений
- Простота внедрения и управления
- Снижение стоимости владения

4 ИТОГОВЫХ СОВЕТА

- Продумайте ваши требования
- Настройка «на вас» обязательна
- Выбирайте решение тщательно
- Ищите партнера, а не поставщика



**Дополнительные вопросы Вы можете
задать по электронной почте
security-request@cisco.com
или по телефону: (495) 961-1410**

CISCO SYSTEMS

