



ИТ-бюллетень Ernst & Young

Содержание

- ▶ Исследование Ernst & Young о роли ИТ в бизнесе
- ▶ Новый выпуск Insights on IT Risk
- ▶ Ряд хакерских атак в мире

Вышло исследование Ernst & Young *Innovating for growth: IT's role in the new global economy*

Стали известны результаты глобального исследования роли ИТ в бизнесе, проведенного Ernst & Young в 15 странах по всему миру. В документе описаны современные приоритеты, которые ставит бизнес перед ИТ. Согласно опросу, больше всего топ-менеджмент компаний ожидает от руководителей ИТ-подразделений понимания требований бизнеса (81% опрошенных). На втором месте стоит коммуникация между ИТ и бизнесом (71%). Следующими ожиданиями, согласно исследованию, являются инициация изменений и инноваций в бизнесе (66%) и управление рисками в ИТ (62%).

Результаты опроса по некоторым позициям анализировались отдельно: в разрезе ответов топ-менеджмента и руководителей ИТ. В частности, бизнес и ИТ разошлись в оценке готовности ИТ соответствовать будущему развитию бизнеса. Только 15% руководителей бизнеса считают ИТ хорошо подготовленным к будущим требованиям бизнеса. В то же время руководители ИТ оценивают свою готовность к будущим вызовам более оптимистично.

Это только часть выводов данного исследования. Ознакомиться с полными результатами можно на веб-сайте нашей компании ([http://www.ey.com/Publication/vwLUAssets/Innovating_for_growth: IT role in the new global economy/\\$FILE/Innovating%20for%20growth%20-%20IT%20role%20in%20the%20new%20global%20economy.pdf](http://www.ey.com/Publication/vwLUAssets/Innovating_for_growth:_IT_role_in_the_new_global_economy/$FILE/Innovating%20for%20growth%20-%20IT%20role%20in%20the%20new%20global%20economy.pdf)).

Отдел услуг в области информационных технологий и ИТ-рисков



**Константин
Невядомский**

Партнер

Kostiantyn.Neviadomskiy@ua.ey.com



Владимир Матвийчук

Менеджер

Volodymyr.Matviychuk@ua.ey.com

Тел: +380 (44) 490 3000

Факс: +380 (44) 490 3030

www.ey.com/ukraine

Вышел очередной выпуск Insights on IT risk: Building control efficiency

Консультационное подразделение Ernst & Young провело анализ способов построения эффективной системы внутренних контролей в организации. Рекомендации для компаний опубликованы в новом выпуске Insights on IT Risk.

Последние 5 лет были очень трудными для тех, кто отвечает за систему внутренних контролей в компаниях. Немало лет потребовалось высшему руководству многих организаций, чтобы встать на ноги после усиления регуляторных требований, таких как Закон Сарбейна-Оксли. Но в 2008 году земля опять ушла из-под ног у руководителей - по причине мирового финансового кризиса. Очередное повышение регуляторных требований заставляет Службу Внутреннего Контроля прилагать все большие усилия. С одной стороны, регуляторы требуют большего соблюдения требований, которые они накладывают на деятельность компаний. С другой стороны, собственники и акционеры компаний ожидают увеличения эффективности деятельности компаний. Руководителям, ответственным за внутренний контроллинг в организации, приходится искусно маневрировать между этими требованиями. Мы считаем, что в данной ситуации необходимо по-новому посмотреть на существующую систему внутренних контролей для ее оптимизации, а возможно и реорганизации.

В данном документе изложено видение того, как компании могут наиболее эффективно оптимизировать существующую систему внутренних контролей. Какие существуют распространенные недостатки в современных системах внутренних контролей, которые можно относительно быстро обнаружить и исправить? Какие шаги следует предпринять компании для оптимизации своей системы внутренних контролей? Полный текст документа можно бесплатно скачать с веб-сайта нашей компании ([http://www.ey.com/Publication/vwLUAssets/Building_controls_efficiency/\\$FILE/Building_controls_efficiency.pdf](http://www.ey.com/Publication/vwLUAssets/Building_controls_efficiency/$FILE/Building_controls_efficiency.pdf)).



В марте произошел ряд успешных кибер-атак на известные компании

18 марта стало известно о проникновении злоумышленников во внутреннюю сеть компании RSA, известного производителя электронных ключей для двухфакторной авторизации. По оценкам IDC, RSA контролирует около 70% данного рынка. Ключи двухфакторной авторизации широко используются частными и государственными организациями для усиления политики доступа к своим информационным ресурсам, в том числе и по удаленному доступу. Утечка внутренней информации в компании не ведет напрямую к компрометации всех электронных ключей, используемых в мире, но с ее использованием возможны злоумышленные действия уже в отношении конечных клиентов RSA.

28 марта появились сведения об успешной атаке на веб-сайты компании SUN, работающие под управлением СУБД MySQL. Сообщается, что в результате атаки был получен доступ к информации о клиентах и сотрудниках компании, а также к пользовательским логинам и хешам паролей.

Данные инциденты в очередной раз напоминают, что программные средства все еще уязвимы, что может быть использовано для доступа к внутренней информации компании. Но кроме технических, также важны и организационные аспекты управления информационной безопасностью в компании. Так, RSA стала жертвой комплексной атаки. Это говорит о том, что злоумышленники обнаружили и использовали недостатки во внутренних процедурах компании. Возможно, сыграл свою роль и человеческий фактор. В случае с MySQL, показателен тот факт, что многие хеши паролей конкретных пользователей были легко дешифрованы, что говорит о слабости самих паролей пользователей, которые использовались в компании. Это является недочетом в организационной работе компании, а не техническими ограничениями компьютерных систем.

В свете случившегося, напоминаем о важности соблюдения требований информационной безопасности в компаниях:

1. Сложные пароли, с активированной блокировкой учетных записей являются хоть и неудобным, но эффективным средством защиты информационных ресурсов в случае подбора паролей третьими лицами;
2. Информирование сотрудников компании об общепринятых формах атак киберпреступников снижает вероятность успешности таких атак. Даже отсутствие технических уязвимостей не спасет компанию, если ее сотрудники будут

разглашать свои логины и пароли на подставных сайтах в результате фишинга.

3. Нельзя пренебрегать антивирусной защитой, но и не стоит ею ограничиваться. Троянские программы-шпионы получают все большее распространение. Также появляются специализированные программы, нацеленные на добывание конкретной информации, например в банках.
4. Процедуры информационной безопасности – это не разовая акция. В сегодняшнем мире угрозы и риски постоянно изменяются, и для успешного противодействия новым рискам необходимо постоянное реагирование. Для крупных компаний эффективно использование специального подразделения, отвечающего за информационную безопасность в компании, а также проведение регулярных аудиторских процедур силами подразделения внутреннего аудита компании.

Два недавних выпуска Insights on IT Risk посвящены информационной безопасности: В данных материалах детально рассматриваются важные аспекты и способы реагирования на действия злоумышленников:

Information security in a borderless world - Time for a rethink([http://www.ey.com/Publication/vwLUAssets/Insights_on_IT_risk_-_Information_security_in_a_borderless_world:_Time_to_re-think/\\$FILE/EY_Insights_on_IT_risks_-_Information_security_in_a_borderless_world.pdf](http://www.ey.com/Publication/vwLUAssets/Insights_on_IT_risk_-_Information_security_in_a_borderless_world:_Time_to_re-think/$FILE/EY_Insights_on_IT_risks_-_Information_security_in_a_borderless_world.pdf)) и Countering cyber attacks ([http://www.ey.com/Publication/vwLUAssets/Countering_cyber_attacks_March2011/\\$FILE/Countering_cyber_attacks_March2011_GL_Adv.pdf](http://www.ey.com/Publication/vwLUAssets/Countering_cyber_attacks_March2011/$FILE/Countering_cyber_attacks_March2011_GL_Adv.pdf)).

Если у вас есть вопросы по любому из отчетов, Владимир Матвийчук готов обсудить их по телефону в Киеве +380 44 499 33 43.