УДК 004.7:004.056

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВИКОРИСТАННЯ КОНЦЕПЦІЇ BYOD В ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Стасівський Л.С., Масальська О.О.
ДВНЗ «Національний гірничий університет» http://bit.nmu.org.ua/, stasivskyj@gmail.com

У сучасній організації робочі місця багатьох співробітників перестають бути статичними. На сьогоднішній день є можливість підключатися до різних хмарних сервісів і використовувати можливості свого пристрою для виконання робочих операцій, буквально тримаючи в руках телефон, адже тепер комп'ютер, який стоїть на столі робітника, вже не має цінності. Маючи можливість виконувати ті ж робочі завдання, але за допомогою свого особистого пристрою, співробітник, як показує практика, буде прагнути це робити. Завдання IT-служби в компанії - забезпечити йому таку можливість.

Ключові слова – технологія Bring Your Own Device; безпека корпоративних даних.

ВСТУП

Концепція BYOD (Bring Your Own Device – Принеси Свій Власний Пристрій) – це підхід до організації робочого місця співробітника, при якому він застосовує власний пристрій для доступу до інформаційних ресурсів компанії.

Наскільки підхід виправдовує свої очікування, можна судити з того, як він активно застосовується в різних компаніях у всьому світі. Наприклад, згідно з дослідженням компанії Fortinet, 74% респондентів регулярно використовують особисті електронні прилади у виробничих цілях. Більш того, 55% з опитаних вважають таке використання особистих приладів своїм правом, а не привілеєм. А, за даними дослідження компанії Microsoft, найбільш лояльними до концепції BYOD є китайські компанії (86%) і найменш лояльними – японські (30 %). На рис. 1 представлено розподіл рівня лояльності компаній в різних країнах до концепції BYOD [1].

Синій (верх): концепція BYOD дозволена і вітається.

Блакитний: концепція BYOD дозволена, але не вітається.

Помаранчевий: концепція BYOD заборонена.

Коричневий (низ): концепція BYOD не регулюється.[1]

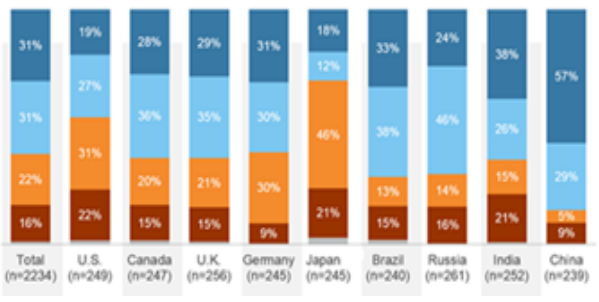

Рисунок 1. Розподіл рівня лояльності компаній в різних країнах до концепції BYOD

При прийнятті рішення про перехід компанії на використанні концепції BYOD необхідно проаналізувати наслідки впровадження данної технології. Особливу увагу потрібно звернути на забезпечення заходів безпеки, оцінити вплив BYOD на всю систему мережевої безпеки компанії, мати уявлення про проблеми які можуть виникнути.

Ноутбуки, планшети, смартфони які підключаються до корпоративні мережі, отримують доступ до веб-додатків і поштових систем, доставляючи чимало проблем IT адміністраторам і фахівцям з інформаційної безпеки.

Найбільш популярними рішеннями проблем інформаційної безпеки є використання інфраструктурі віртуальних робочих місць VDI (Virtual Desktop Infrastructure - Віртуальні Робочі місця), використання технології MDM (керування мобільними приладами).[2]

ВИКОРИСТАННЯ ВІРТУАЛЬНИХ РОБОЧИХ МІСЦЬ

Для вирішення поставлених завдань необхідно застосування гнучких збалансованих методів, замість заходів по повній забороні мобільних пристроїв в корпоративному середовищі.

Використання інфраструктури віртуальних робочих місць VDI (Virtual Desktop Infrastructure – віртуальні робочі місця) – віртуальні робочі місця, засновані на серверних рішеннях, представляють із себе користувальницькі додатки або цілі операційні системи, що працюють у віртуальному середовищі, під управлінням адміністратора, функціонуючого на централізованому сервері. Один фізичний сервер, на якому розгорнуте віртуальне середовище, може одночасно працювати з безліччю віртуальних робочих місць користувача, розгорнутих на його віртуальних машинах. Число одночасно підтримуваних віртуальних машин залежить від кількості пам'яті і обчислювальних ресурсів фізичного сервера. Такий підхід дуже зручний, оскільки забезпечує централізоване адміністрування і зберігання даних, дозволяє поступово нарощувати інфраструктуру, і, в міру необхідності, створювати, або видаляти робочі місця, а також легко переносити їх з одного сервера на інший. Перевагою застосування таких віртуальних робочих місць є високий захист корпоративних даних у віртуальному середовищі, надаючи, при цьому, користувачу високу свободу дій, відкриваючи доступ до корпоративних IT-ресурсів через захищене

з'єднання, що запобігає витоку конфіденційних даних на пристроях користувачів.[3]

ВИКОРИСТАННЯ ДОДАТКІВ УПРАВЛІННЯ МОБІЛЬНИХ ПРИСТРОЇВ

Додатковим рішенням даної проблеми інформаційної безпеки є використання спеціального інструментарію для управління мобільними пристроями (MDM). Дана технологія за рахунок розмежування доступу MDM повинна була допомогти знайти баланс між перевагами працівників і потребою компаній захистити корпоративні дані організації, які впровадили MDM. Компанії що ввели цю технологію доходять висновку, що це ПЗ негативно позначається на досвіді користувача. По-перше, установка на особистий апарат деякий фрагмент коду, за допомогою якого можливо відправляти будь-які команди і настройки, викликає неприйняття персоналу. По-друге, смартфони та планшети спочатку розроблялися під споживчий сегмент, тобто з урахуванням максимальної зручності використання, і їх власники просто не готові миритися з появою яких недоліків.

MDM - далеко не єдиний інструмент, який дає можливість організувати роботу з персональними пристроями в корпоративному середовищі. Багатьом компаніям під силу обійтися і без нього, за рахунок онлайнових сервісів (у тому числі дистанційного видалення даних).[4]

ЗАГРОЗА ВТРАТИ МОБІЛЬНИХ ДАНИХ

Найбільша загроза для мобільних даних - крадіжка або втрата самого апарату, але для її вирішення існує безліч недорогих і навіть безкоштовних інструментів (Find My iPhone, Where's my Droid, пр.). Наприклад, компанії можуть використовувати безкоштовну утиліту Apple iOS Configuration Utility і каталог AppleID для автоматичної настройки Find My iPhone на користувацьких апаратах, а щоб не дати злодію відключити пристрій - застосовувати Device Restrictions. Звичайно, з обережністю, адже помилкові спрацьовування не виключені.

ВИСНОВОК

При впровадженні даної технології потрібно дотримуватися перерахованих вище методів вирішення проблеми інформаційної безпеки, а також для покращення захищеності корпоративних даних можливо застосовувати:

- Двуфакторную аутентифікацію.
- Безпечний віддалений доступ з допомогою SSL VPN.
- Підтримка обізнаності персоналу.

BYOD – це лише концепція, перехідна форма між класичним нерухомим комп'ютером на робочому столі і новим підходом до організації роботи з метою забезпечити максимальний комфорт і продуктивність працівника, давши йому можливість працювати там, тоді й таким чином, як йому буде зручно.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. BYOD – четыре буквы способные напугать даже крупную компанию (Електрон. ресурс) / Спосіб доступу: URL: http://vido.com.ua/article/3112/byod-chietyrie-bukvy-sposobnyie-napughat-dazhie-krupnuiu-kompaniiu/ - BYOD – четыре буквы способные напугать даже крупную компанию.
2. Что такое BYOD и насколько она эффективна в организациях? (Електрон. ресурс) / Спосіб доступу: URL: http://ecm-journal.ru/post/Chto-takoe-BYOD-i-naskolko-ona-ehffektivna-v-organizacijakh.aspx - Что такое BYOD и насколько она эффективна в организациях?
3. Bring Your Own Device с точки зрения интересов отечественного бизнеса (Електрон. ресурс) / Спосіб доступу: URL: http://www.cisco.com/web/RU/news/releases /txt /2012/112912c.html - Bring Your Own Device с точки зрения интересов отечественного бизнеса
4. Инфраструктура виртуальных ПК (Електрон. ресурс) / Спосіб доступу: URL: http://www.parallels.com/ ru/solutions/vdi/ - BYOD – Инфраструктура виртуальных ПК
5. Управление основными данными (Електрон. ресурс) / Спосіб доступу: URL: http://ru.wikipedia.org/wiki – Управление основными данными.