УДК 004.054

**Полтавець А.І.,**
**Моденов Ю.Б.,** к.т.н.

# ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ МЕРЕЖІ ПІДПРИЄМСТВА «КРАЙТЕК»

Національний авіаційний університет

modenov1951@gmail.com

*Ефективний захист IT-інфраструктури та прикладних корпоративних систем сьогодні неможлива без впровадження сучасних технологій контролю мережевого доступу. Часті випадки крадіжки носіїв, які містять цінну інформацію ділового характеру, все більше змушують приймати організаційні заходи*

**Ключові слова:** гіпервізор, сервер додатків, мережевий екран, спам-листи

## *Вступ*

Актуальність даної статті визначається високим рівнем проблем інформаційної безпеки навіть в умовах стрімкого зростання технологій та інструментальної бази для захисту даних. Неможливо забезпечити стовідсотковий рівень захисту корпоративних інформаційних систем, при цьому коректно розставляючи пріоритети в завданнях із захисту даних в умовах обмеженості частки бюджету, спрямованої на інформаційні технології. Надійний захист обчислювальної та мережевої корпоративної інфраструктури є базовим завданням в області інформаційної безпеки для будь-якої компанії.

## *Огляд міжнародного стандарту ISO/IEC17799*

Стандарт *ISO/IEC17799* є найпоширенішим на сьогоднішній день інструмент де-факто, щодо керування інформаційної безпеки. Він використовується в 27 країнах світу. *ISO/IEC*17799 – це збірка практичних рекомендацій, яка дає деталізоване керівництво щодо розробки, впровадження та оцінки заходів керування інформаційною безпекою, а також загальні принципи побудови систем контроля інформаційної безпеки. Оскільки компанія «Крайтек» займається розробкою програмного забезпечення та орієнтована на зовнішній ринок, вона повинна відповідати міжнародним стандартам в області мережевої безпеки. Керуючись стандартом ISO/IEC17799 та беручи до уваги структуру та особливості побудови мережі компанії «Крайтек». Було розглянуто такі пункти стандарту, які забезпечать продуктивну та відмовостійку роботу компанії

## *Аналіз структурної схеми мережі компанії «Крайтек»*

Розглянемо детально структуру мережі та сервіси необхідні для забезпечення стабільної роботи компанії (рис.1).

Гипервізор або монітор віртуальних машин – програма або апаратна схема, що забезпечує або дозволяє одночасне, паралельне виконання декількох операційних систем на одному і тому ж хост-комп'ютері.

Сервер додатків – сервер, на якому виконуються прикладні програми.

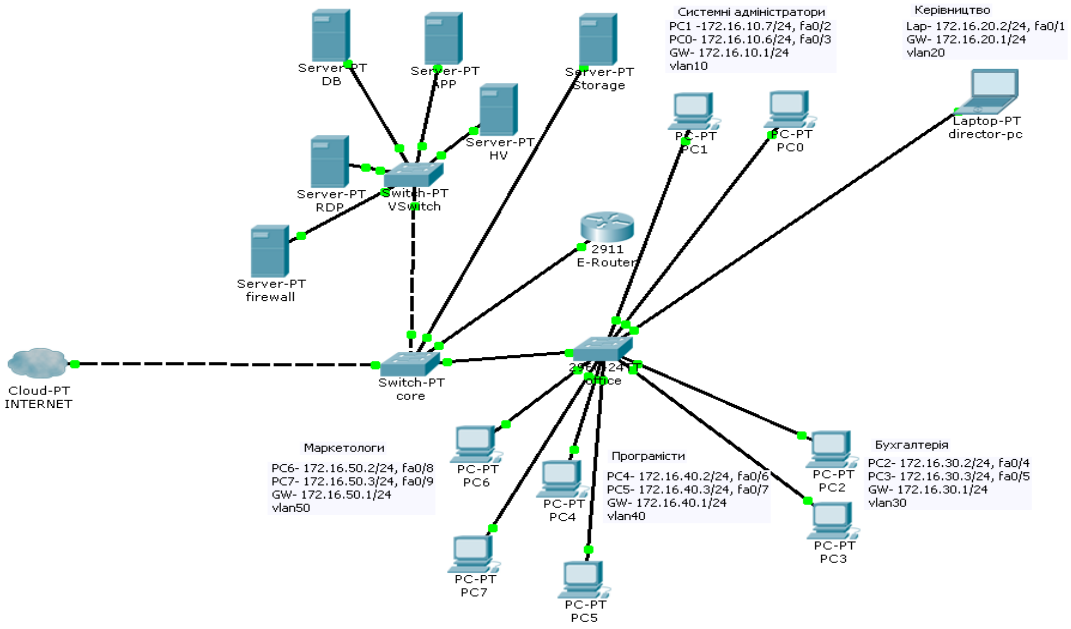


Рис.1. Схема локальної мережі компанії «Крайтек»

На сервері додатків запущені такі сервіси:

- *Apache HTTP* – сервер для роботи внутрішніх web-сайтів компанії.
- *Trac* – вільний браузерний застосунок для управління проектами.
- *ERP*-система (*task*) – планувальник задач.

Сервер баз даних – займається обслуговуванням та управлінням базою даних, відповідає за цілісність і збереження даних, а також забезпечує операції введення-виведення при доступі клієнта до інформації.

На сервері БД запущені такі сервіси:

- *MySQL* – система керування реляційними базами даних. Зберігаються дані від *ERP*-системи, дані внутрішніх веб-сайтів.

- *PostgreSQL*- об'єктна-реляційна система керування базами даних (СКБД). База даних бухгалтерії.

*RDP*- Протокол віддаленого робочого столу) - пропріетарний протокол прикладного рівня, що використовується для забезпечення віддаленої роботи користувача з сервером, на якому запущений сервіс термінальних підключень.

Основна задача *RDP*:

- Запуск бухгалтерської програми 1С.
- Забезпечення роботи віддалених працівників.

Мережевий екран – комплекс програмних засобів, здійснює контроль і фільтрацію мережевих пакетів які проходять через нього відповідно до заданих правил.

Для організації продуктивної роботи фірми встановлений окремий сервер - сховище даних storage де зберігаються віртуальні жорсткі диски для серверу віртуалізації. Як бачимо з (рис.1.) в компанії є 2 комутатори (*office-sw ma core*). В *office-sw* на пряму підключені офісні працівники. *Core* служить для з'єднання офісного свіча, серверів та маршрутизатора.

Також в core включений інтернет-канал провайдера який надає компанії «Крайтек» вихід в глобальну мережу Інтернет.

### *Недоліки виявлені в мережевих налаштуваннях компанії «Крайтек»*

Всі офісні працівники знаходяться в одній мережі 192.168.10.0/24, що являється не дуже надійним рішенням з точки зору мережевої безпеки, оскільки будь-який співробітник знаходячись на своєму робочому місці та знаючи логін і пароль ресурсу може отримати інформацію, доступ до якої йому заборонений. Це може призвести до розповсюдження конфіденційних даних.

Також було зафіксовано численні скарги від офісних працівників на низьку працездатність ПК. В ході аналізу даної проблеми було виявлено, що на робочих станціях є велика кількість ресурсозатратних і не потрібних для роботи програм. Що й призводить до утилізації оперативної пам'яті і як наслідок низької швидкодії ПК. В ході аналізу було виявлено несвоєчасне оновлення антивірусного програмного забезпечення, що призводить до розповсюдження програм-вірусів.

Переглянувши журнал подій на сервері *FW*, було помічено неодноразові *DdoS* -атаки на мережу компанії. Проаналізовавши який саме тип атак використовується, було помічено, що *DdoS* здійснюється через відкриті *icmp* порти.

Працівникам компанії часто приходять спам-листи. Оскільки електронна пошта останнім часом стала головним каналом поширення шкідливих програм. Спам забирає масу часу на перегляд і подальше видалення повідомлень, викликає у співробітників почуття психологічного дискомфорту. Разом зі спамом нерідко видаляється важлива кореспонденція, що може призвести до втрати клієнтів, зриву контрактів та інших неприємних наслідків.

Доступ до всіх внутрішніх ресурсів компанії здійснюється через сервер *RDP*. Реалізується це за допомогою підключення по протоколу *ssh*. Враховуючи, що *ssh* порти постійно відкриті, працівник має можливість цілодобового доступу до обладнання. Відкритий для всіх мереж *ssh* порт є однією з причин здійснення несанкціонованого доступу до внутрішньої мережі компанії.

З плином часу годинники комп'ютерів мають тенденцію відставати. *Network Time Protocol* – мережевий протокол часу (*NTP*) є одним із способів вести точний час. Багато сервісів Інтернет спираються або сильно залежать від точності годин комп'ютерів. Наприклад, веб-сервер може отримувати запит на посилку файлу, який був недавно модифікований. У локальній мережі необхідно, щоб годинники комп'ютерів, які спільно використовують файли, були синхронізовані, щоб час модифікації файлів встановлювалося правильно. Такі служби, як *cron*, також залежать від правильності установки системних годин, оскільки запускають команди в певний час. Таким чином важливо мати актуальні *NTP* сервери. Дана служба запущена на сервері *FW*. Перевіривши налаштування було виявлено, що синхронізація часу здійснюється з *NTP* сервером, який уже давно не підтримується, що призводить до певних незручностей, таких як не вірно указані в часі події у лог-файлах служб.

Оскільки компанія має нештатних працівників, існує необхідність в листуванні для передачі інформації. Було зафіксовано випадки, коли конфіденційна інформація потрапляла до конкурентів і цим самим завдавала значної шкоди для роботи компанії.

### *Вдосконалення мережевих налаштувань враховуючи виявлені недоліки на підприємстві «Крайтек»*

Для забезпечення контролю доступу було розділено мережу на підмережі з метою виключення можливості потрапляння на ПК іншого відділу при відомому логіні та паролі. Дана ціль досягається при здійсненні таких налаштувань:

1) Розділено всю мережу на підмережі – це допоможе в майбутньому за до-

помогою *ACL* розмежовувати трафік офісних працівників.

2) Також було використано такий інструмент як *vlan* для розділення локальної мережі на віртуальні підмережі. Кожна підмережа знаходиться в окремому *vlan'i*. Трафік маркується на порту свіча куди включений кожний ПК. Всі відділи мають різні номер *vlan*.

3) Для уникнення розповсюдження не бажаної інформації між працівниками, було розділено всю мережу на підмережі, та сформовано *ACL* листи, за допомогою яких забороняється трафік між відділами. На кожен відділ створюється окремий *access*-лист, який потім прикріплюється на сабінтерфейс підрозділу. Відділу IT дозволяється мати доступ до всіх підмереж. Всім іншим дозволити доступ до серверів *FW, APP* та *RDP*. При таких налаштуваннях трафік не буде проходити між відділами, як наслідок працівник який знає логін та пароль ПК співробітника іншого підрозділу не зможе віддалено зайти на його робочу станцію, оскільки трафік з іншої підмережі буде забороненим.

Для підвищення швидкодії робочих станцій працівників, було змінено тип облікових записів з «адміністратора» на «звичайний доступ». Обліковий запис користувача – це зібрання інформації, яку *Windows* використовує для визначення, до яких файлів і папок має доступ користувач і які зміни на комп'ютері він може здійснювати. Також у ньому зберігаються особисті налаштування. Кожен користувач отримує доступ до свого облікового запису за допомогою імені користувача та пароля. Стандартні облікові записи призначені для щоденного користування комп'ютером та не дають право на встановлення додаткових програм. Обліковий запис адміністратора надає повний контроль над комп'ютером. Зміна типу облікового запису здійснюється засобами Windows.

Встановленовлено ліцензійне антивірусне програмне забезпечення *Eset NOD*32.

Для збільшення надійності підключення до термінального сервера було створено тунель *ssh*. *Ssh* тунель - це тунель, створюваний за допомогою ssh з'єднання і використовується для шифрування тунельованих даних. Застосовується для захищеної передачі інформації в мережі Інтернет. Особливість полягає в тому, що незашифрований трафік будь-якого протоколу шифрується на одному кінці *ssh* з'єднання і розшифровується на іншому.

Для зменшення кількості спроб отримання несанкціонованого доступу до ресурсів компанії, було реалізовано можливість підключення до сервера *RDP* та інших внутрішніх систем з зовнішніх мереж лише в робочі години. Винятком являється лише відділ IT, який має доступ до всіх ресурсів 24/7 для можливості адміністрування мережі. Реалізоване дане рішення на сервері *FW* засобами встроєного брандмауера *iptables* операційної системи Linux. По замовчуванню *iptables* забороняє будь-який трафік з мережі та в мережу, тому для доступу в Інтернет написано правило для відкриття трафіку в двох напрямках. Оскільки дане рішення не є правильним з точки зору мережевої безпеки, було дозволений доступ в Інтернет лише в робочі години. Винятком являються *IP*-адреси: 193.124.123.12 та 187.13.56.29, які належать системним адміністраторам мережі. Правила вмикаються та вимикаються в визначений час. Реалізовано це за допомогою служби *cron*. Регулярні дії описуються інструкціями, поміщеними в файли *crontab* і в спеціальні директорії. Створено теку */etc/ufwrules* в якій знаходяться файли *block.sh* та *allow.sh* з правилами . В файлі *allow.sh* описано правило за допомогою надбудови *iptables ufw*, яке відкриває з'єднання з зовнішніми мережами. Виконується він службою *cron* з понеділка по п'ятницю з 09:00 до 18:00.

Для забезпечення більш надійного захисту інформації для кожного користувача було створено персональний аккаунт. Дане рішення реалізовано засобами

*Windows Serwer* 2003. Здійснені налаштування дозволяють виявити, ким із працівників були внесені зміни в документи. Також це забезпечує гнучке управління правами облікових записів. При звільненні працівника достатньо вимкнути його аккаунт, а не змінювати пароль групового облікового запису, як це робилося раніше.

Для уникнення *DdoS*-атак, які здійснюються через відкриті *icmp* порти, було заборонено *icmp ping* запити.

Для усунення спаму, який засмічує поштову скриньку користувача, і цим самим знижує швидкість опрацювання корисних листів на поштовому сервері налаштовується *DNSBL*. Поштовий сервер звертається до *DNSBL*, і перевіряє в ньому наявність *IP*-адреси клієнта, з якого він приймає повідомлення. При позитивній відповіді вважається, що відбувається спроба прийому спам-повідомлення. Серверу відправника відправляється помилка 5xx (невиправна помилка) і повідомлення не приймається. Поштовий сервер відправника створює «відмовне повідомлення» відправнику про неможливість доставки пошти. Фільтри спаму значно зменшують непродуктивні трудовитрати, пов'язані з розбором спаму, знижують трафік і завантаження серверів, покращують психологічний фон в колективі і зменшують ризик залучення співробітників компанії в шахрайські операції. Крім того, фільтри спаму зменшують ризик зараження новими вірусами, оскільки повідомлення, що містять віруси часто мають ознаки спаму. На сервері *FW* налаштований поштовий сервер *postfix* в конфігураційному файлі якого підключаються *DNSBL*–списки.

Для зменшення ризику несанкціонованого доступу було встановлено програму *fail2ban*. Основна ідея *Fail2ban* - при перевищенні 6-ти невдалих вводів пароля поспіль блокує IP, з якого були спроби підбору пароля на заданий час. Налаштована дана служба на сервері *FW*.

Враховуючи той факт, що кожному працівнику був виданий власний логін та пароль, виникла необхідність ведення журналу подій сервера *RDP*. Для того, щоб система записувала в журнал подій інформцію про те, хто входить в систему, потрібно налаштувати групові політики, а саме включити параметри аудиту системи, що відносяться до подій входу в систему. Події входу в систему відстежують події як локального, так і мережевого входу. Кожна подія містить інформацію про обліковий запис, за допомогою якої зроблений вхід в систему, а також час, коли ця подія відбулася. Засобами *Windows Serwer* 2003 було ввімкнено аудит входу в систему, аудит доступу до об’єктів та аудит подій входу в систему.

Синхронізація годин є дуже важливою умовою, оскільки *ssh* доступ в компанії «Крайтек» дозволяється працівникам фірми в визначений час, враховуючи той факт що в налаштуваннях використовувалися *NTP* сервери, які вже не обслуговуються виникла необхідність в зміні *NTP* сервера на актуальний. Також було указано декілька *NTP* серверів для забезпечення надійності правильної синхронізації часу, навіть у випадку відмови одного із указаних *NTP* серверів.

Для підвищення мережевої безпеки та виключення можливості потрапляння конфіденційної інформації до конкурентів, було налаштовано шифрування поштових повідомлень.

Шифрування дозволяє захистити інформацію шляхом її перетворення в незрозумілий текс з можливістю подальшого розшифрування. Всі працівники компанії для відправки та прийому пошти використовують поштовий клієнт *Mozilla Thunderbird*, в якому встановлений зовнішній палагін *Enigmail* для шифрування та дешифрування листів на основі створених криптографічних ключів додатком *Kleopatra*. За допомогою якої створюється публічний ключ, який відсилається отримувачу пошти, за допомогою якого шифрується повідомлення. У власника ключа залишається закритий ключ, яким він користується для дешифрування листа, який йому був адресований.

### *Висновки*

Питання безпеки завжди стояло перед комп'ютерними мережами, але сьогодні як ніколи зростає усвідомлення того, наскільки важливою є безпека комп'ютерних мереж в корпоративних інфраструктурах. В даний час для кожної корпоративної мережі необхідно мати чітку політику в області безпеки. Ця політика розробляється на основі аналізу ризиків, визначення критично важливих ресурсів і можливих загроз.

Враховуючи наведені вище фактори в компанії «Крайтек» виникла необхідність дослідження та удосконалення власних мережевих налаштувань. В даній статті продемонстровано аналіз існуючої мережі, показано недоліки та можливі наслідки нехтування стандартами безпеки.

Для забезпечення повної безпеки всієї IT інфраструктури необхідно впроваджувати механізми захисту на всіх рівнях мережі від кордону до комутаторів доступу. На рівні доступу рекомендується використовувати керовані комутатори з підтримкою функціонала захисту протоколів *ARP, DHCP, STP*. Авторизувати користувачів при підключенні за допомогою технології 802.1*x*. Підключати співробітників в різні *VLAN* залежно від їх функціональних обов'язків і задавати правила взаємодії і доступу до різних ресурсів на рівні розподілу.

Для управління всім мережевим обладнанням повинні використовуватися захищені протоколи *SSH, HTTPS, SNMPv3*. Для можливості аналізу логфайлів час на пристроях має бути синхронізоване. Для розуміння, який трафік ходить в мережі, наскільки завантажено обладнання, які події на ньому відбуваються, використовувати протокол *Syslog*.

### *Список літератури*

1. Організація ISO и IEC «ISO і IEC, ISO_IEC_17799_2000_rus», Самара: Изд-во СПбГУЕФ, 2008. – 150 с.

2. Блінов А.М. «Інформаційна безпека: Навчальний посібник. Частина 1 ». - СПб.: Изд-во СПбГУЕФ, 2010. – 96 с.

3. Горбатов В. С, Полянська О. Ю. Г67 «Основи технологій шифрування». - М .: Гаряча лінія-Телеком, 2004. – 248 с.

4. Петренко С.О., Володимир А. Курбатов В. А. «Політики безпеки компанії при роботі в Інтернет» видавництво СПбГУЕФ, 2008. – 150 с.

Статтю подано до редакції 23.03.2015