Асоціація малих міст УКРАЇНИ

СУПЕРМАРКЕТ РІШЕНЬ для громад

ICWR INSTITUTE OF CYBER WARFARE RESEARCH

CyberLab Комп'ютерна криміналістика

Технічне налаштування IT-інфраструктури громади

План зустрічі

01 Роль IT-інфраструктури в діяльності територіальної громади

02 Побудова мережевої інфраструктури

03 Серверна інфраструктура

04 Робочі станції та облікові записи

05 Захист інформаційної інфраструктури

06 Резервне копіювання та відновлення

07 Захист електронної пошти та вебресурсів

08 Практичні рекомендації

Роль IT-інфраструктури в діяльності територіальної громади

- **Забезпечення надання послуг:** Безперебійна робота ЦНАП, доступ до державних реєстрів у режимі.
- **Захист критичних масивів даних:** Безпечне зберігання та обробка персональних даних мешканців, фінансової та земельної документації.
- **Єдиний робочий простір:** Надійна взаємодія між центральним офісом та віддаленими філіями.
- **Відповідність нормативній базі:** Виконання вимог законодавства у сфері захисту інформації.

Побудова мережевої інфраструктури

Внутрішній периметр

Логічна сегментація

Жорстке ізолювання критичних вузлів (ЦНАП, фінанси, сервери, відеоспостереження, гостьовий Wi-Fi).

Контроль доступу на рівні портів

Впровадження 802.1X та Port Security (захист від підключення несанкціонованих пристроїв у розетки).

Захист базових протоколів

DHCP Snooping та ARP Inspection для запобігання атакам типу Man-in-the-Middle та підміни шлюзу всередині мережі.

Маршрутизація між сегментами

Використання Access Control Lists (ACL). Заборона прямого зв’язку між клієнтськими машинами (Client Isolation).

Побудова мережевої інфраструктури

Зовнішній периметр

Політика «Default Deny»

Блокування всього вхідного і вихідного трафіку, крім явно дозволеного. Обмеження доступу до нестандартних портів зсередини.

Захист віддаленого доступу

Категорична заборона прокидання портів служб RDP, SMB, баз даних назовні.

Шифрування трафіку

Побудова Site-to-Site VPN (IPsec) для зв'язку зі старостатами; Client-to-Site VPN для віддалених працівників.

Відмовостійкість

Балансування навантаження та автоматичне перемикання на резервного провайдера без розриву сесій.

Серверна інфраструктура

- **Тотальна віртуалізація:** Використання гіпервізорів. Відмова від розгортання ОС безпосередньо на залізі.
- **Відмовостійкість:** Побудова кластерів. Забезпечення живої міграції віртуальних машин між фізичними нодами без зупинки сервісів у разі апаратного збою.
- **Ізоляція ролей:** Принцип «одна задача — одна ВМ». Категорична заборона суміщення критичних ролей.
- **Незалежне керування:** Використання виділених інтерфейсів управління (iLO, iDRAC) у власному ізольованому VLAN без доступу з інтернету.
- **Дискові підсистеми:** Використання надійних масивів (апаратні RAID або програмний ZFS).

Облікові записи та управління доступом

~Централізована інфраструктура

Відмова від Workgroup. Єдина точка автентифікації та управління життєвим циклом користувачів.

~Принцип найменших привілеїв

Тотальне відкликання прав локальних адміністраторів у рядових працівників.

~Захист привілейованих записів

Автоматична генерація унікальних паролів локального адміністратора для кожного ПК із їх зберіганням в AD. Захист від атак типу Pass-the-Hash.

~Жорсткі парольні політики

Блокування облікових записів після N невдалих спроб вводу (захист від брутфорсу). Заборона використання тривіальних паролів.

Робочі станції та політики безпеки кінцевих точок

~Контроль периферії через GPO

Блокування довільних USB-накопичувачів. Використання білих списків (за VID/PID) ексклюзивно для захищених носіїв (КЕП/ЕЦП).

~Обмеження виконання софту

Дозвіл на запуск додатків виключно з директорій Windows та Program Files (або за хешем/ сертифікатом).

~Стандартизація робочого середовища

Примусове блокування екрана. Автоматичне підключення мережевих дисків та принтерів через GPO.

~"Stateless PC" та Patch Management

Заборона зберігання робочих документів на локальних накопичувачах. Централізоване розгортання критичних патчів безпеки (WSUS).

EDR & SIEM

Перехід на EDR

Сигнатурний аналіз базових антивірусів **неефективний** проти загроз нульового дня та безфайлових атак.

EDR виконує моніторинг дерева процесів, ін'єкцій у пам'ять та нетипового використання легітимних утиліт.

EDR можна налаштувати на **миттєве відключення скомпрометованого хоста від мережі** із залишенням лише каналу для розслідування.

Централізований збір логів

Зловмисник із правами адміністратора в першу чергу **зачищає журнали подій** Windows/Linux.

Впровадження SIEM забезпечує **збір логів** з Active Directory, фаєрволів, серверів та мережевого обладнання **в режимі реального часу**.

Налаштування тригерів на ланцюжки подій.

Інтеграція з месенджерами для миттєвого реагування на критичні інциденти.

IDS/IPS & Vulnerability Management

IDS/IPS

Глибокий аналіз пакетів (DPI) забезпечує перевірку вмісту мережевого трафіку на льоту, а не лише портів та IP-адрес.

Системи виявлення та запобігання (Snort / Suricata) блокує відомі експлойтів, спроб SQL-ін'єкцій та звернень до командних серверів (C2) зловмисників.

Fail2Ban, динамічні ACL автоматично додають IP-адресу атакуючих до чорних списків (захист від Brute-force та DDoS).

Vulnerability Management

Використання **автоматизованих сканерів** для інвентаризації мережі.

Перевірка інфраструктури на відповідність стандартам безпеки **(CIS Benchmarks)** та наявність дефолтних паролів.

Виявлення критичних CVE у встановленому ПЗ на серверах та комутаторах.

Резервне копіювання та відновлення

- **Правило 3-2-1:** 3 копії даних, 2 різних носії, 1 копія поза межами локації. Впровадження незмінних сховищ, де беккап неможливо змінити чи видалити навіть з правами root.
- **Тотальна ізоляція:** Сервер резервного копіювання категорично заборонено вводити в загальний домен. Він повинен мати унікальні облікові дані і знаходитись у власному ізольованому VLAN.
- **Спеціалізовані рішення:** Використання Proxmox Backup Server, Veeam Backup & Replication або BorgBackup для інкрементального копіювання на рівні блоків та дедуплікації.
- **Метрики RPO та RTO:** Чітке визначення для кожного сервісу: скільки даних ми можемо втратити (RPO) і як швидко маємо відновити роботу (RTO).
- **Тестування копій:** Резервна копія не існує, поки ви з неї успішно не відновилися. Налаштування автоматичного тестування відновлення у віртуальній пісочниці.

Захист електронної пошти

Автентифікація DNS: Обов'язкове впровадження SPF (хто має право відправляти), DKIM (криптографічний підпис листа) та DMARC. Поступовий перехід DMARC на політику p=reject (відхиляти всі підробки).

Шлюз безпеки (SEG): Весь вхідний та вихідний трафік проходить через проміжний вузол. Перевірка вкладень у пісочниці, блокування макросів та архівів із паролями.

Транспортне шифрування: Примусове використання TLS для з'єднань між серверами. Заборона використання застарілих протоколів (нешифрованих портів 25, 110, 143).

Захист доступу скриньок: Використання багатофакторної автентифікації (2FA) для доступу. Обмеження доступу за гео-IP.

Захист вебресурсів

Приховування інфраструктури: Проксіювання трафіку через Web Application Firewall. Блокування DDoS-атак на рівнях L3/L4/L7 та фільтрація ботів.

Ізоляція локального сервера: Налаштування локального фаєрвола на вебсервері так, щоб він приймав підключення (порти 80/443) виключно від пулу IP-адрес WAF.

Захист адміністративних панелей: Обмеження доступу до адмін-панелей на рівні вебсервера. Вхід дозволено лише через корпоративний VPN або з чіткого білого списку IP-адрес.

Hardening та HTTP-заголовки: Примусове використання HTTPS. Впровадження заголовків безпеки (Content-Security-Policy, X-Frame-Options) для захисту від XSS-атак та клікджекінгу.

Практичні рекомендації: інфраструктура на Open-Source

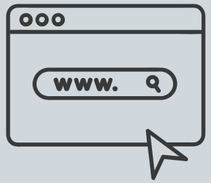
- **Firewall:** OPNsense або pfSense. (Маршрутизація, VLAN, IDS/IPS Suricata, Multi-WAN, WireGuard/IPsec VPN).
- **Віртуалізація:** Proxmox VE. (Кластеризація, ZFS-масиви, ізоляція сервісів у LXC/KVM, жива міграція — альтернатива VMware ESXi).
- **Управління доступом:** Samba AD DC/Windows Server AD. (GPO, авторизація Windows-машин, керування користувачами).
- **Резервне копіювання:** Proxmox Backup Server. (Інкрементальні беккапи на рівні блоків), UrBackup (Повноцінні бекапи).
- **Моніторинг та SIEM:** Zabbix (моніторинг стану мережі та заліза) + Wazuh (SIEM та безкоштовний EDR на робочі станції).
- **Пошта та Веб:** Proxmox Mail Gateway, eFa Project (захист від спаму/фішингу) + HAProxy / Nginx Proxy Manager (Reverse proxy для ізоляції вебсервісів).

Що можна зробити зараз?

- Зайдіть на Shodan або візьміть Nmap і проскануйте свою зовнішню IP-адресу. Закрийте всі відкриті порти, переведіть усе на VPN.
- Заберіть права адміна: Переведіть користувачів у режим звичайних Users. Це зупинить левову частку загроз.
- Підніміть тестовий стенд: Візьміть старий ПК, поставте туди Proxmox і спробуйте розгорнути якийсь із інструментів які сьогодні розглянули.

Як звернутися до служби підтримки кібербезпеки

Служба підтримки - це швидкий доступ до фахової допомоги у сфері кібербезпеки



Заповнити звернення на сайті Супермаркет рішень для громад

через кнопку «Звернутися до служби підтримки» на сайті supersolution.net.ua

Отримати зворотній зв’язок

АСОЦІАЦІЯ МАЛИХ МІСТ УКРАЇНИ

СУПЕРМАРКЕТ РІШЕНЬ для громад

ICWR INSTITUTE OF CYBER WARFARE RESEARCH

CyberLab Комп'ютерна криміналістика

Служба підтримки

+38 (096) 380 17 39, +38 (093) 477 50 67