Author: Nechytailenko Anna

Research work №1 : Zero trust approach for remote workers on public WiFi networks.

Executive Summary and Threat Model

- **Context and destruction of the Castle-and-Moat mode**: The traditional concept of the "corporate perimeter" assumed that inside the organization's network, all devices are trusted, and protection focuses on external borders (such as firewalls). The "Work from Anywhere" paradigm completely negates this approach. When a remote worker uses uncontrolled networks (such as public Wi-Fi), corporate data and accesses are physically taken to a hostile environment where the network layer is a priori compromised, giving Assume Breach's security analysis even more attention.
- **Threat Actors and motivation:**
  - Cybercriminals: Act with a clear financial motivation. The main purpose of — is to steal corporate credentials, session access tokens or intellectual property for further sale on the Dark Web or deploy targeted attacks (for example, Ransomware) on the company's infrastructure.
  - Script Kiddies: Located in the same physical location. Their motivation ranges from petty hooliganism and skill testing to opportunistic data collection through untargeted traffic interception.
- **Модель загроз (Threat Model):** У середовищі відкритого Wi-Fi критичній небезпеці піддаються два компоненти тріади CIA: *конфіденційність* (витік даних) та *цілісність* (модифікація даних у транзиті). Основні вектори атак:
  - *Фальшиві точки доступу (Evil Twin):* Створення зловмисником точки доступу з легітимною назвою (SSID) для примусового маршрутизування трафіку працівника через своє обладнання.
  - *Атаки Man-in-the-Middle (MitM) та ARP-spoofing:* Перехоплення, читання та зміна трафіку між ноутбуком жертви та справжнім шлюзом мережі.
  - *Сніфінг трафіку:* Пасивне прослуховування радіоефіру для перехоплення нешифрованих пакетів.
- **Threat Model**: In an open Wi-Fi environment, two components of the CIA triad are critically endangered: confidentiality (data leakage) and integrity (data modification in transit). Main attack vectors:
  - Fake Access Points (Evil Twin): An attacker creates a Legitimately Named Access Point (SSID) to force routing of an employee's traffic through their equipment.
  - Man-in-the-Middle (MitM) and ARP-spoofing attacks: Intercepting, reading and changing traffic between the victim's laptop and the real network gateway.
  - Traffic Sniffing: Passive listening to the radio airwaves to intercept unencrypted packets.

Core Analysis: go from Castle-and-Moat model to Zero Trust approach

Network Layer compromise and VPN security illusion

In traditional enterprise infrastructure, the network layer is tightly controlled by administrators: configured switches, VLAN segmentation, and physical hardware protection create a zone of trust. However, the concept of "Work from Anywhere" transports the employee to a public Wi-Fi environment, where the network layer (L2 and L3 according to the OSI model) is a priori considered hostile and compromised. The organization has no control over routing, switching or physical access to the router in the coffee shop. This creates ideal conditions for traffic interception attacks or DNS manipulation.

Historically, virtual private networks (VPNs) have been used to solve this problem. However, a classic VPN is no longer a panacea because it follows the outdated logic of giving broad trust. If the remote worker's end device is compromised (for example, by downloading malware at the host level), the connected VPN client will simply create a secure, encrypted tunnel for the attacker directly into the internal corporate network. This lead to the violation of the Principle of Least Privileges (PoLP), as a classic VPN usually gives a connected device wide trust access to entire subnets or even the entire corporate infrastructure, instead of granular access exclusively to the only application or service that an employee needs to perform the current task. Having received such excessive visibility of the internal network, an attacker or malicious software from a compromised laptop can freely scan other internal servers for vulnerabilities and spread freely within the infrastructure, namely lateral movement.

Архітектура нульової довіри (ZTA) та принцип Assume Breach

У відповідь на ці виклики сучасна кібербезпека перейшла до **Архітектури нульової довіри (Zero Trust Architecture, ZTA)**. Фундаментальна зміна полягає в тому, що довіра більше не базується на IP-адресі, фізичному місцезнаходженні чи факті підключення до певної мережі (навіть VPN). Головний постулат ZTA: *"Ніколи не довіряй, завжди перевіряй"*. Кожна спроба доступу до ресурсу розглядається як потенційно ворожа, поки не буде доведено протилежне.

Основою цього підходу є концепція **Assume Breach** (припускаємо, що злам уже стався). Ми свідомо виходимо з того, що публічна Wi-Fi мережа (L2/L3) вже контролюється зловмисником, який сніфить або маніпулює маршрутизацією трафіку. Відповідно, ми припиняємо покладатися на безпеку базової мережі і переносимо механізми захисту на вищі рівні моделі OSI — **транспортний (L4)** та **рівень застосунків (L7)**.

Застосування ешелонованої оборони (Defense in Depth) для віддаленого працівника

Оскільки єдиного "магічного" рішення не існує, для захисту віддаленого працівника застосовується **Ешелонована оборона (Defense in Depth)**. Якщо зловмисник долає один рівень захисту (наприклад, перехоплює трафік у публічній мережі), інші рівні мають зупинити атаку.

Zero Trust Architecture (ZTA) and Assume Breach Principle

In response to these challenges, modern cyber security has moved to the Zero Trust Architecture (ZTA). A fundamental change is that trust is no longer based on an IP address, physical location, or the fact that you connect to a specific network (even a VPN). ZTA's main postulate is "Never trust, always check". Each attempt to access the resource is treated as potentially hostile until proven otherwise.

The basis of this approach is the concept of Assume Breach which assumes that the hack has already occurred. We deliberately assume that the public Wi-Fi network (L2/L3) is already controlled by an attacker who sniffs or manipulates traffic routing. Accordingly, we stop relying on core network security and move protection mechanisms to higher levels of the OSI — transport (L4) and application (L7) models.

Application of echeloned defense (Defense in Depth) for a remote worker

Since there is no single "magical" solution, Echeloned Defense is used to protect the remote worker. If an attacker overcomes one level of protection (for example, intercepts traffic on the public network), then by the given approach the other levels must stop the attack.

1. **Identity Layer**: Since we can no longer trust the network to which the employee is connected, the main barrier of protection is strict verification of his identity (Identity and Access Management, IAM). Using only a traditional login and password is a critical vulnerability: due to fake public Wi-Fi, an attacker can easily redirect a user to a fake login page and lure their credentials (for example, carry out a phishing attack). To mitigate this risk, Zero Trust requires mandatory multi-factor authentication (MFA). The use of modern MFA methods, such as biometrics or physical hardware keys (for example, the FIDO2 standard), guarantees resistance to such threats. For instance, during authorization, the system asks the user to tap the key. The FIDO2 standard works so that the key cryptographically checks the real address of the site on which the user is located. If the key "sees" that it is not a real corporate portal (for example, microsoft.com), but a hacker double (for example, m1crosoft.com), it simply refuses to generate access code. Thus, even if a hacker tricks an employee's password on an uncontrolled network, he will not be able to log in, because the hardware key cannot be fooled by visual forgery of the site.
2. **Host Layer**: In the Zero Trust concept, the end device becomes an autonomous micro-perimeter capable of independently repelling attacks in enemy networks. This protection is provided by three components:
   - 2.1. OS Hardening: Minimize the attack surface by disabling unnecessary services, closing vulnerable ports, and using a local firewall.
   - 2.2. Least Privilege Principle (PoLP): Work exclusively without local administrator rights. This creates a critical barrier: even if a malicious file is launched, the threat remains isolated in the user space and cannot make irreversible changes at the level of the system kernel space or disable security measures.
   - 2.3. EDR (Endpoint Detection and Response) systems: Continuous behavioral monitoring is used instead of outdated signature antiviruses. If EDR captures an anomaly (such as an attempt to mass encrypt files), the system instantly blocks the process and automatically cuts off the compromised device from accessing corporate resources.
3. **Data Layer:** The key principle of protection at this — level of data must remain unreadable for the attacker under any conditions, whether it is a complete interception of traffic in a public Wi-Fi network or a physical loss of the device. This is implemented through strict technical enforcement in two dimensions:
   - 3.1. **Data in Transit:** In the Zero Trust model, the company abandons the single corporate VPN tunnel in favor of ZTNA (Zero Trust Network Access) solutions. Traffic security here is guaranteed by two parallel processes:
     - 3.1.1. Micro-segmentation of connections: Instead of letting the user inside the corporate network, the ZTNA agent on the laptop creates individual, isolated encrypted tunnels exclusively to those individual applications that are needed for work. All other infrastructure remains invisible.
     - 3.1.2. Architectural blocking of open traffic: The company at the gateway level prohibits any unencrypted connections. Servers are configured to automatically reject any network request that does not use modern cryptographic protocols (such as TLS 1.3). Thanks to this, End-to-End Encryption becomes an non-alternative requirement for data transmission.
   - 3.2. **Data at Rest:** Working in public places creates a high risk of physical theft of the laptop. Mandatory full-disk encryption (BitLocker for Windows, FileVault for macOS) is used to protect local files. To control this, the company uses device management systems (MDM — Mobile Device Management). A strict compliance policy applies

through MDM: if the system records that the employee voluntarily turned off BitLocker, the device instantly receives the status of "non-compliant" and the ZTNA agent automatically breaks all connections and blocks access to servers until the disk is encrypted again.

Strategic Recommendations

Based on the principles of risk management and the Zero Trust architecture, it is proposed to implement the following effective solutions. The use of a risk-oriented approach allows the company not to spend resources to protect everything in a row, but to focus on critical threat vectors.

Risk-oriented approach:

- Immediate action (Critical risk): Categorically prohibit access to critical corporate resources without continuous rigorous device health checks (Device Posture Check) and identity verification through MFA.
- Risk Acceptance: Allow connection to public Wi-Fi networks without using a corporate VPN exclusively for isolated web surfing of non-critical public resources. Mandatory condition: the device must be securely insulated by a rigidly configured local firewall.

Corporate and technical recommendations:

- Appliance of ZTNA: Complete rejection of legacy VPNs in favor of Zero Trust Network Access solutions to provide granular access at the level of individual applications.
- Automation (DevSecOps approach): Setting up an automated OS and software update process on end devices. This guarantees prompt closure of known vulnerabilities (CVE elimination) even before the employee leaves to work in the

List of used sources:

- **Syllabus**
- **miniOrange. (n.d.). *ZTNA vs VPN: Understanding the Shift in Secure Access*. Аналітичний огляд архітектурних відмінностей між мережевим доступом та мікро-сегментацією. Отримано з: https://www.miniorange.com/blog/ztna-vs-vpn/**
- **FIDO Alliance. (n.d.). *FIDO Specifications*. Офіційна технічна документація стандартів апаратної багатофакторної аутентифікації (FIDO2 / WebAuthn) та захисту від фішингу. Отримано з: https://fidoalliance.org/specifications/**
- **DevSecOps School. (n.d.). *CVE (Common Vulnerabilities and Exposures) in DevSecOps: A Comprehensive Tutorial*. Огляд управління вразливостями та автоматизації оновлень безпеки на кінцевих пристроях. Отримано з: https://devsecopsschool.com/blog/cve-common-vulnerabilities-and-exposures-in-devsecops-a-comprehensive-tutorial/**
- **TechTarget. (n.d.). *What is full-disk encryption (FDE)?* Технічний опис принципів захисту даних у стані спокою (Data at Rest) та апаратного шифрування. Отримано з: https://www.techtarget.com/whatis/definition/full-disk-encryption-FDE**