Root of Trust (Źródło Zaufania) to zaufana strona trzecia lub komponent, który gwarantuje bezpieczeństwo i autentyczność nowego połączenia lub systemu.

Przykłady:

HSM - hardware sec module - zewnętrzny sprzęt przeznaczony do przechowywania kluczy, certyfikatów, credentiali kryptograficznych bezpiecznych na dużą skalę.

TPM - trusted platform module - wbudowany chip. Posiada wbudowaną ochronę przeciw burtę force. Może towarzyszyć FDE (full disc encryption).

Secure Enclave - IOS; is isolated from the main processor to provide an extra layer of security and is designed to keep sensitive user data secure even when the Application Processor kernel becomes compromised. Monitoruje boot process, create a true random numbers, store root cryptogtwphy Keys, and more.

CA - Wystawia certyfikaty SSL/TLS, które potwierdzają tożsamość stron internetowych.

Access Control types:

RBAC - Role-Based AC, IT different access, Management different access.

Discretionary Access Control - dostęp przyznawany przez ownera. User creates a file, user assign level of Access.

Mandatoty (many security level: public, private, secret) each file - different security level and each user - different security level

Rule - based (gdy jest spełniony warunek: określona pora dnia, wymagana konkretna przeglądarka)

Mail Antyspoofing:

DMARC - wydaje dyspozycje na podstawie SPF i DKIM. Czy mail ma trafić do spamu czy nie.

SPF - czy mail pochodzi z autoryzowanego servera.

DKIM - czy wiadomość nie została zmodyfikowana. System, który podpisuje maile cyfrowo, aby potwierdzić że wiadomość pochodzi z autentycznej domeny. Receiver potwierdza podpis cyfrowy wysyłającego kluczem publicznym, który jest w rekordzie DNS.

NAC

Network Access Control - system bezpieczeństwa, który sprawdza czy zostały spełnione określone warunki przed połączeniem z internetem np. czy jest poprawna konfiguracja firewalla lub czy OS jest zaktualizowany.

RPO (Recovery Point Objectives) - define how much data loss is acceptable during recovery.

RTO (Real Time Obejctives) - określa ile czasu potrzeba do naprawy, żeby usługa znów działała.

SIEM - Sec Info and Event Manag - Service; Log aggregator.

IPSec - related with VPN.

Escalation scripting - using to automation and orchestration, related with Incident Respons.

Docs:

Statement of Works - tasks.

SLA - service provider will provide 99% uptime
(SLA - minimum terms for provider services).

Data retention - policy data preservating. How long data must be storaged np. Regulacje Unijne

Due CARE - należyta staranność (np. Sprawdzanie czy serwery są właściwie zabezpieczone lub podczas penetration testing).

What to do with a RISK?

Accept - risk acceptance in business

Transfer - transfering risk out of organisation

Risk- avoidance - disconnecting from the internet

Risk tolerance - acceptable amount of risk.

Mitigation - np. Offline backups - ransomware mitigations

Shadow IT - ignoring IT policies, example: using private Google disc for corporate data

Quarantine (antivirus) - moving to the safe area.

IPS - allow or deny disposition based on known vulnerabilities.

>Fail Open- gdy IPS przestaje działać, ruch sieciowy jest nadal przepuszczany

Side loading - instalacja apek manualnie spoza Apple App Store.

Vendor monitoring - proces ciągłego monitorowania dostawców

Regulatory compliance - przestrzeganie przepisów i norm, np. Unijnych

Attestation- formalne potwierdzenie czy coś jest zgodne z normami

Self assesment - samoocena firmy
Internal self-assessment
An internal self-assessment with audit can verify users have the correct permissions and all users meet the practice of least privilege.

Dependency list - to plan for any potential chang

Policy administrator - to generate Access token or credentails

Gap analisys - where we are & where we want to be.

Parrarel processing - use multiple procesors

Snapshot - type of backup on VM

Screened subnet - strefa zdemilitaryzowana (DMZ).

SCAP security contrnt automatom protocol - automatyzacja podatności

Exposure factor - calculate the business loss in %

Procent oceny ryzyka. Jeśli w wyniku pożaru spłonęły 40% budynku to exposure factor = 40%.

RAID - technologia łączenia dysków twardych w jedną logiczną całość. Not a backup technology.

Right to audit - added to business contracts to ensure access to periodic audits when working with third party.

Vendor monitoring - obserwacja usługodawcy. Np. Audyty usług.

Due dilligence - proces certyfikowania informacji przed zrobieniem biznesu z drugą firmą.

Conflict of interest - personal and famili relations in business.

Something you have:
+Karta rfid
+Token generator (!)

Data Loss Prevention - can idenify and block sensitive data sending in the network. (emails)
Malware stole all data (also sensitive) from mail. — solution DLP

Data Sovereignty - not moving data outsider the origin country (suwerenność danych)

Geographical dispersion - rozproszenie geograficzne. Np centra w różnych krajach.

How to block keylogger?
Block all unknown outbound network traffic

Credentials could not be validated = No Proper certificat installed

Chain of custody - proces dokumentowania dowodów, zapewnia integralność bo dokumentuje także każdego kto miał styczność z dowodami.

E-Discovery - collection of digital docs (maile jakoś dowód)

Legal hold - technika utrzymania dokumentów. Firma otrzymuje wezwanie do sądu, więc IT blokuje maile przed usunięciem.

Non repudiation- gwarantuje, że akcja miała miejsce i kto ją wykonał.

WAF Web App Fw - firewall to protect web based apps. Filtruje w czasie rzeczywistym kto co wpisuje.

VPN CONCENTRATOR - central connectivity point for all remote VPN.

UTM UNIFIED THREAT MAMAGMENT - jakiś kolejny firewall

XDR - identyfy malicious software and Attacks. Extended detenction and response.

Sase - Cloudf awarie version of VPN

HIPS - host based IPS

Simple network management protocol- provide alerts and alarm from server and infrastructure devices
End of life - no longer supported by vendor

Embedded system- not provide Access to OS, not provide method of upgrading firmware. Np. Time clock.

Industrial Control system - **ICS** to systemy, które wspierają funkcjonowanie infrastruktury przemysłowej, zapewniając jej niezawodność, bezpieczeństwo i efektywność działania.

Enumeracja - zbieranie Informacji

Access point umożliwia bezprzewodowy dostęp do sieci lokalnej. Umożliwia adresom łączenie się ze sobą.

Net flow logs - software: Summarum of network traffic
(np. Czy ataker użył skompromitowanego urządzenia do poruszania się między systemami).

In band - przekazywanie kluczy tym samym kanałem co komunikacja np. whatsapp

Out of band - poza głównym kanałem.SMS, spotkanie

Removing affected servers from the network - eradiction

Role przy obrocie danymi:

Data controller - zajmuje się procesami danych. Np. Dział płac

Data owner - kierownik działu HR. Zarządza danymi.

DATA subject - każda osoba której dane są przetwarzane (shipping adres)

Processor - third party Company wykonująca zadania controllera. Tylko wykonuje polecenia. Np. Administrator it.

Data custodian - manage permissions to data

Access Control List - implemented in routers to allow or restrict Access devices np. Sieciowy Dostęp do data center.

Stakeholders managment - zarządzanie interesariuszami - np. Zarządzanie różnymi grupami w czasie budowy biura (pracownicy korpo , budowlańcy, inwestorzy, władze lokalne..)

Retention policies- jak długo dane mają być backupowane

Change managment - zarządzanie zmianą - **Zarządzanie zmianą** to proces planowania, wdrażania i monitorowania zmian w organizacji.

Bloatware - dziwne aplikacje intalowane przed sprzetażą sprzetu.
Preinstalowane przez producenta. Np. Health lub Compass na iOS.

Regulatory Pentest - obligacja do pentestow - np. W hipppa (Health insurance portable acts) lub PCI dss (płatności kartą), lub iso 127001, lub gdpr (generał data protection - regulacje w UE).

Loss:

SLE - single loss. Utrata komputera to 100 zł. SLE = 100 zł. (hint: E jako Euro)

ARE - annual rate - 7 laptopów w rok

ALE - all events cost in 1 Year. (hint: E jako Euro)

Key streaching - kilkuktotnu hash

Software defined Wan- direclty Access CloudKit, from all corporate locationa

802.1x - autentication with corporare credentials when connecting to the network

VPN - use corporate laptop in coffee shops and hotels

Replay attack- przechwytywanie i retrasnmitowanie danych na server. Packets captures.

W kontekscie apli /acji webowych, HA
osiąga się przez:

1. Redundancję - Uruchamianie aplikacji na wielu serwerach (np. w chmurze lub w centrze danych), co oznacza, że jeśli jeden serwer przestanie działać, inny przejmie jego zadania.

2. Load balancing (równoważenie obciążenia) - Rozkładanie ruchu użytkowników na kilka serwerów, co zapewnia równomierne obciążenie i eliminuje ryzyko przeciążenia pojedynczego serwera.

3. Failover - Mechanizm automatycznego przełączenia na zapasowy serwer lub infrastrukturę, gdy główny serwer przestaje działać.

4. Monitorowanie i automatyczne odzyskiwanie - Systemy monitorujące stan aplikacji i serwerów

Geolocation
Geolocation would allow the system to assign rights and permissions based on physical location. In this question, there's no documentation on where users are located and how those locations could be used for access control.

Wymiana kluczy Diffiego-Hella (Diffie-Hellman). Jest to protokół kryptograficzny umożliwiający bezpieczną wymianę kluczy przez niezabezpieczony kanał komunikacyjny. Celem tego algorytmu jest umożliwienie dwóch stron, które wcześniej nie miały wspólnego klucza, wygenerowanie wspólnego sekretu (klucza) używanego do szyfrowania komunikacji.

OSI

Model OSI (Open Systems Interconnection) to teoretyczny model, który opisuje, jak komputery komunikują się w sieciach. Jego celem jest podzielenie tego procesu na 7 warstw, aby łatwiej było zrozumieć, jak dane przepływają przez sieć od jednego urządzenia do drugiego.

Przykład na co dzień:

Chcesz wysłać wiadomość przez WhatsApp.

1. Warstwa aplikacji: Piszesz wiadomość w aplikacji.
2. Warstwa prezentacji: Wiadomość jest szyfrowana (np. dla bezpieczeństwa).
3. Warstwa sesji: WhatsApp tworzy połączenie między Twoim telefonem a telefonem znajomego.
4. Warstwa transportu: Wiadomość jest podzielona na małe fragmenty (pakiety).
5. Warstwa sieci: Pakiety są wysyłane przez różne ścieżki w internecie.
6. Warstwa łącza danych: Dane są przesyłane przez karty sieciowe i routery.
7. Warstwa fizyczna: Przesył odbywa się przez kable lub fale Wi-Fi.

Model OSI pomaga specjalistom od IT lepiej zrozumieć i naprawiać problemy w sieciach, bo każdy problem można przypisać do konkretnej warstwy.

THM how web works

Oto wyjaśnienie kroków z Twojego schematu w prosty sposób, krok po kroku:

1. Wpisanie adresu (np. tryhackme.com) w przeglądarce

To moment, gdy wprowadzasz adres strony w pasku przeglądarki. Twoje urządzenie chce się dowiedzieć, gdzie (na którym serwerze) znajduje się ta strona.

2. Sprawdzenie lokalnej pamięci podręcznej (cache)

Twój komputer najpierw sprawdza, czy już zna adres IP tej strony (czy odwiedzałeś ją wcześniej).

- Jeśli zna adres, korzysta z niego bez dalszych zapytań.
- Jeśli nie, idziemy dalej.

3. Sprawdzenie serwera DNS Twojego dostawcy internetu

Twój komputer pyta serwer DNS (książkę adresową internetu) dostawcy internetu, czy zna adres IP tej strony.

4. Zapytanie do serwera głównego DNS (root server)

Jeśli Twój serwer DNS nie zna odpowiedzi, wysyła pytanie do głównego serwera DNS (root server).

- Root server wie, gdzie znaleźć więcej szczegółowych informacji o domenie (np. tryhackme.com).

5. Serwer autorytatywny DNS odpowiada

Autorytatywny serwer DNS (taki, który zarządza konkretną stroną) zwraca adres IP serwera, na którym znajduje się ta strona internetowa.

6. Przejście przez Web Application Firewall (WAF)

Twoje żądanie (np. „pokaż mi stronę tryhackme.com") trafia do zapory ogniowej aplikacji internetowych.

- Zapora sprawdza, czy Twoje żądanie nie jest złośliwe, np. czy nie próbujesz zaatakować strony.

7. Przejście przez Load Balancer (równoważnik obciążenia)

Równoważnik obciążenia kieruje Twoje żądanie do jednego z wielu serwerów, które obsługują stronę.

- Dzięki temu strona działa szybko, nawet jeśli korzysta z niej wiele osób naraz.

8. Połączenie z serwerem na porcie 80 lub 443

Twoje żądanie dociera do wybranego serwera.

- **Port 80** to połączenie nieszyfrowane (HTTP).
- **Port 443** to połączenie szyfrowane (HTTPS).

9. Serwer odbiera żądanie „GET"

Serwer rozumie, że chcesz pobrać stronę (HTML) i wysyła odpowiedź.

10. Serwer kontaktuje się z bazą danych

Jeśli strona wymaga danych z bazy (np. Twojego konta użytkownika), serwer pobiera je w tle.

11. Przeglądarka wyświetla stronę (renderowanie)

Przeglądarka odbiera dane (HTML, CSS, JavaScript) i tworzy z nich widoczną stronę internetową, którą widzisz na ekranie.

Cały proces zajmuje zaledwie kilka sekund! Każdy z tych kroków dzieje się błyskawicznie, dzięki czemu widzisz stronę niemal natychmiast po wpisaniu jej adresu. Jeśli coś jest niejasne, daj znać!

Binarny

- dlaczego w systemie dziesiętnym

Adres **255.255.255.0** to adres w formacie **notacji dziesiętnej**, używanej w maskach podsieci IPv4. Każda z czterech liczb (oktetów) jest reprezentowana jako 8-bitowa wartość binarna.

Przeliczamy każdy oktet na system binarny:

Dziesiętnie Binarnie

255 11111111

255 11111111

255 11111111

0 00000000

Wynik w systemie binarnym:

255.255.255.0 → 11111111.11111111.11111111.00000000

Jest to typowa **maska podsieci /24**, oznaczająca, że pierwsze 24 bity adresu IP są używane do identyfikacji sieci, a pozostałe 8 bitów do identyfikacji hostów.

XSS HTML example

Oczywiście, poniżej przedstawiam kilka przykładów użycia znacznika <a> z atrybutem href w języku HTML:

1. **Link do zewnętrznej strony internetowej:**

Odwiedź Przykład.com

Opis: Ten kod tworzy hiperłącze prowadzące do strony “https://www.przyklad.com” z tekstem “Odwiedź Przykład.com”.

2. **Link do innej strony w ramach tej samej witryny (link względny):**

Skontaktuj się z nami

Opis: To hiperłącze prowadzi do strony “kontakt.html” znajdującej się w tej samej domenie. Użycie linków względnych jest przydatne przy tworzeniu odnośników wewnątrz tej samej witryny.

3. **Link do konkretnej sekcji na tej samej stronie:**

Przejdź do Sekcji 1

Opis: Ten link prowadzi do elementu na tej samej stronie, który ma identyfikator id="sekcja1". Jest to przydatne do tworzenia odnośników do określonych części długich stron.

4. **Link otwierający nową wiadomość e-mail:**

Wyślij do nas e-mail

Opis: Po kliknięciu w ten link otworzy się domyślny klient poczty e-mail z wypełnionym polem adresata “kontakt@przyklad.com”.

5. **Link otwierający stronę w nowej karcie:**

Otwórz Przykład.com w nowej karcie

Opis: Atrybut target="_blank" powoduje otwarcie linku w nowej karcie przeglądarki.

6. **Link z atrybutem** title**:**

Strona Główna

Opis: Atrybut title dodaje dodatkową informację, która pojawia się jako podpowiedź (tooltip) po najechaniu kursorem na link.

7. **Link do numeru telefonu:**

Zadzwoń do nas

Opis: Po kliknięciu w ten link na urządzeniu z funkcją telefonowania, zostanie wybrany numer telefonu “+48 123 456 789”.

8. **Link uruchamiający skrypt JavaScript:**

Kliknij mnie

Opis: Ten link uruchamia skrypt JavaScript, który wyświetla okno alertu z wiadomością “Witaj!”.

Pamiętaj, że poprawne i przemyślane użycie znaczników <a> oraz atrybutu href jest kluczowe dla tworzenia intuicyjnych i dostępnych stron internetowych.

Bufferoverflow

- provides artacker
- repeatably
- NOT simple to exploit

fgets wykonuje bound checking

Podsumowanie:

· Niezabezpieczony kod: Użycie funkcji gets ( ) pozwala na wprowadzenie dowolnej liczby znaków, co stwarza ryzyko nadpisania pamięci i ataku typu Buffer Overflow.

· Zabezpieczony kod: Użycie funkcji fgets () sprawia, że program kontroluje długość wprowadzanych danych, co zabezpiecza przed nadpisaniem pamięci poza buforem.

W ten sposób zabezpieczony kod jest odporny na ataki Buffer Overflow!