12 Problematika bezpečnosti počítačových sítí

Wednesday, 19 January 2022 09:10

Fyzická bezpečnost, sociální inženýrství, zranitelnost, exploit, hrozba
Podvržení adres, zesilovač, DoS, DDoS, Man in the Middle (MITM), průzkumné útoky
Malware, trojský kůň, virus, červ, Botnet (zombie), ransomeware
Zabezpečení přepínače (včetně port security) proti zranitelnostem (ARP flooding, DHCP snooping a
starvation,,VLAN, STP, CDP)
Zabezpečení koncových zařízení včetně bezdrátových

- fyzická bezpečnost
  a. zamezení přístupu nepovolených osob k síťovým prvkům
  b. ochrana sítě před fyzickými vlivy
     i. živelné pohromy
     ii. regulace teploty, vlhkost
  c. kamerový dozor
  d. autentizace
  e. separace datových záloh
- sociální inženýrství
  - komunikační metoda, která uživatele přinutí vyzradit určitou informaci
  - snaží se o maximální úroveň důvěryhodnosti
  - např. phishing, jiná URL nebo chyby ve strojovém kódu
- škodlivý software
  - malware
    - zastřešující název pro úmyslně škodlivý softwre
    i. adware
       □ zobrazení nechtěných reklam
    ii. spyware
       □ shromažďování informací
       □ jako keylogger, sledovač souborů, v obrazovkách a kamerách
       □ není jednoduché určit přesnou hranici (cookies, cílená reklama)
    iii. ransomware
       □ blokace systému a zašifrování
       □ vyžadování výkupného (obvykle v kryptoměnách) za dešifrování dat
    iv. virus
       □ vytváří kopie sebe samého
       □ může se přenášet i mezi zařízeními
    v. červ
       □ oproti viru se šíří sám (většinou po síti) nezávisle na hostiteli
       □ rozesílá kopie sebe samého
  - exploit
    - využívá programátorskou chybu v kódu
    - obvykle úmyslem nainstalovat malware a chybu neodhalovat
  - DoS (*Denial of Service*)
    - útok na síťové služby
    - co nejvíce požadavků na určitý stroj (typicky webserver)
    - DDoS (*Distributed DoS*)
       □ rozdělení požadavků mezi více zařízení
       □ těžší na odhalení než DoS kvůli distribuci síťových požadavků
       □ Botnet
          ◆ síť infikovaných počítačů (zombies) řízená centrálně z jednoho místa
          ◆ využívají se mimo DDoS i k posílání spamu
  - man-in-the-middle

        - odposlech komunikace mezi dvěma konci
        - úprava komunikace za účelem vydávání se za druhý konec
- síťové hrozby
    a. MAC flooding
        - zaplavení MAC adresami za účelem vyčerpání paměti switche
    b. DHCP starvation
        - útočník opakovaně posílá DHCP requesty, aby se vyčerpal DHCP pool
    c. DHCP spoofing
        - útočník se vydává za default gateway nebo DNS
        - man-in-the-middle
- zabezpečení síťových prvků
    a. Port Security
        - ochrana proti MAC floodingu
        - vypnutí nepoužívaných portů
        - určení povolených MAC adres na portu
    b. DHCP Snooping
        - ochrana proti DHCP starvation a spoofingu
        - na switchi lze nastavit trusted a untrusted porty, které neumožní posílat DHCP request
- zabezpečení bezdrátových sítí
    - 802.1X
        - standard popisující zabezpečení přístupu do sítě
        - obvykle používá RADIUS protokol pro autentifikaci
            - využívá se u WPA-Enterprise a WPA2-Enterprise
    - AAA
        - *Authentication* - identita uživatele
        - *Authorization* - přístupová práva
        - *Accounting* - metriky využití zdrojů uživatelem na síti
    a. kontrola MAC adres
        - AP obsahuje seznam povolených MAC adres
    b. WEP
        - statické klíče symetrické šifry
    c. WPA
        - stejné klíče jako WEP, ale jsou dynamicky měněny
        - Personal (PSK - *Pre-shared Key*)
            - nevyžaduje autentifikační server
        - Enterprise
            - vyžaduje autentifikační server pro připojení s uživatelským jménem a heslem
    d. WPA2
        - AES šifrování - vyšší výkon - potřeba novějšího zařízení