
# *Raccomandazioni* per una *port filtering policy* comune

Workshop CCR 2021 – 24/5/2021

Luca Carbone per il Gruppo Security

# Considerazioni generali

- tutte le *well known port* TCP/UDP non strettamente necessarie all'erogazione *motivata e documentata* di specifici servizi infrastrutturali **devono** essere chiuse in ingresso (possibilmente in modalità *drop*) sul router di frontiera o sul firewall perimetrale per tutti gli indirizzi non coinvolti nell'erogazione dei corrispondenti servizi;
- tutte le porte transienti (> 1023) **dovrebbero** essere chiuse in ingresso;
- alcune specifiche porte **devono obbligatoriamente** essere chiuse perché espongono servizi intrinsecamente insicuri, datati o che ha senso erogare in sicurezza solo in ambito locale (*SNMP*).

# porte da chiudere

- UDP
  - 7, 19, 21, 69, 111, 141, 161, 162, 3300, 6789
- TCP
  - 21, 23, 109, 110, 111, 123, 135, 139, 143, 161, 162, 389, 445, 515, 631, 636, 1080, 1433, 1434, 1443, 2049, 2301, 2381, 3283, 3300, 3306, 3389, 5432, 5900, 5988, 6789, 8000, 8008, 8443, 8080, 8081, 8888, 9100
- nel caso sia *necessario* aprire una delle porte sopra citate, questo deve essere implementato con opportuni filtri/ACL sull'indirizzo IPv4/IPv6 di provenienza, limitando l'erogazione del servizio a indirizzi IP o sottoreti che necessitino accedervi oppure - ove fattibile - raccomandando l'accesso tramite tramite VPN.

# porte da regolamentare

- UDP
  - 53, 88, 123, 1812, 1813
- TCP
  - 22, 25, 53, 80, 88, 443, 465, 587, 993, 995
- le porte sopra elencate (ssh, SMTP, domain, HTTP/HTTPS, radius, NTP, kerberos, SMTP over SSL, submission , POPS, IMAPS) **devono** essere aperte solo per i server ufficialmente designati all'erogazione dei corrispondenti servizi; la porta *ssh* in particolare non dovrebbe essere aperta per tutti gli indirizzi della LAN ma solo per il *bastion host*, e su quest'ultimo andrebbero implementati meccanismi di mitigazione di attacchi *brute-force* e DoS.

# Gestione eccezioni

- Nelle considerazioni introduttive si è posto l'accento sul fatto che l'erogazione di specifici servizi debba essere *motivata* e *documentata;*
- In quest'ottica il gruppo ritiene ovviamente che le sezioni *siano libere* di derogare alle raccomandazioni esposte, ma che le eccezioni debbano essere:
  - **giustificate**
  - **documentate**
  - **oggetto di revisione in sede di procedura di auditing annuale.**
- Altrimenti detto: una stampante raggiungibile dalla rete geografica deve diventare una *non conformità* che il direttore si impegna a fare correggere.