Valutazione della Sicurezza Informatica della rete interna del Comune di Vicenza

Analisi, criticità e soluzioni

Città di Vicenza

Contenuti

- Analisi della Rete
- Report delle criticità
- Soluzioni e progetti

Analisi della Rete

- **VULNERABILITY ASSESSMENT**
  - Analisi della sicurezza della rete interna al Comune di Vicenza
  - Eseguita nel 2013 da Yarix Srl

  - Analisi approfondita sulla rete, eseguita senza arrecare danno
  - Non è stato condotto un vero attacco (*penetration test*)

Ambito e modalità di analisi

- Gray Box Analysis
  - L’attaccante e l’attaccato sono a conoscenza della tipologia di test
  - L’attaccante ha conoscenza del sistema da attaccare

- Test limitato alla rete privata e svolto dall’interno della rete stessa

Ambito e modalità di analisi

- **Canale**:
  - Rete LAN
  - Rete Wireless
- **Target** :
  - Segmenti di rete IP da analizzare, concordati preventivamente
- **Vector**:
  - Indirizzi IP usati dal pc di test

Verifiche eseguite

- Aggiornamenti dei sistemi operativi e del software
- Vulnerabilità note
- Share di rete non protette
- Password banali o di default
- Traffico anomalo generato da virus

Verifiche eseguite

- Inserimento in rete di PC estraneo
  - Quantità di informazioni acquisibili
  - LAN policy (*access data, password policy, internet access policy*)
  - Log audit (analisi dei log disponibili)
- Ricerca di reti wi-fi non autorizzate agganciate alla rete comunale

Verifiche eseguite

- Scansione di 3870 indirizzi IP
- 975 dispositivi connessi

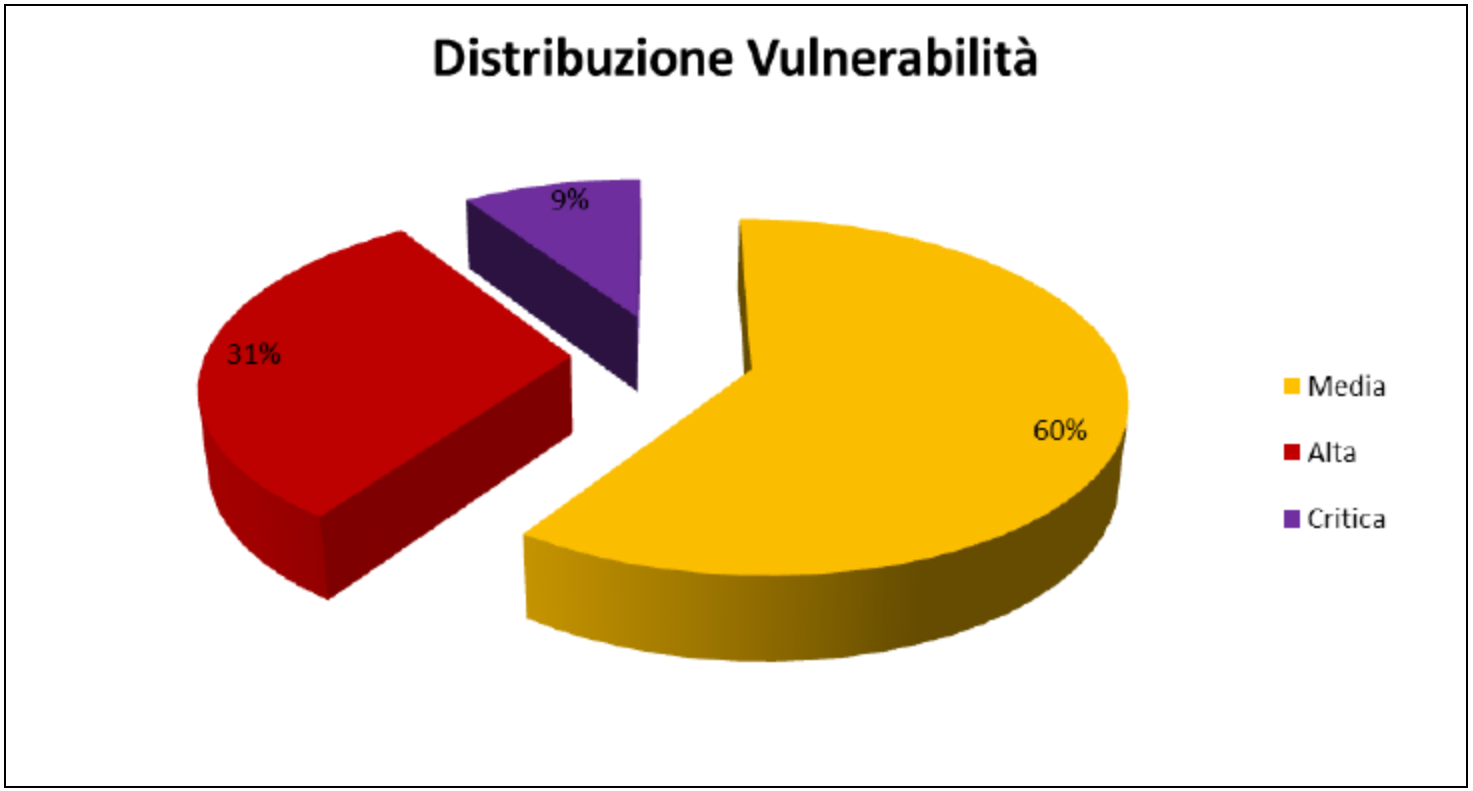
Classificazione delle vulnerabilità

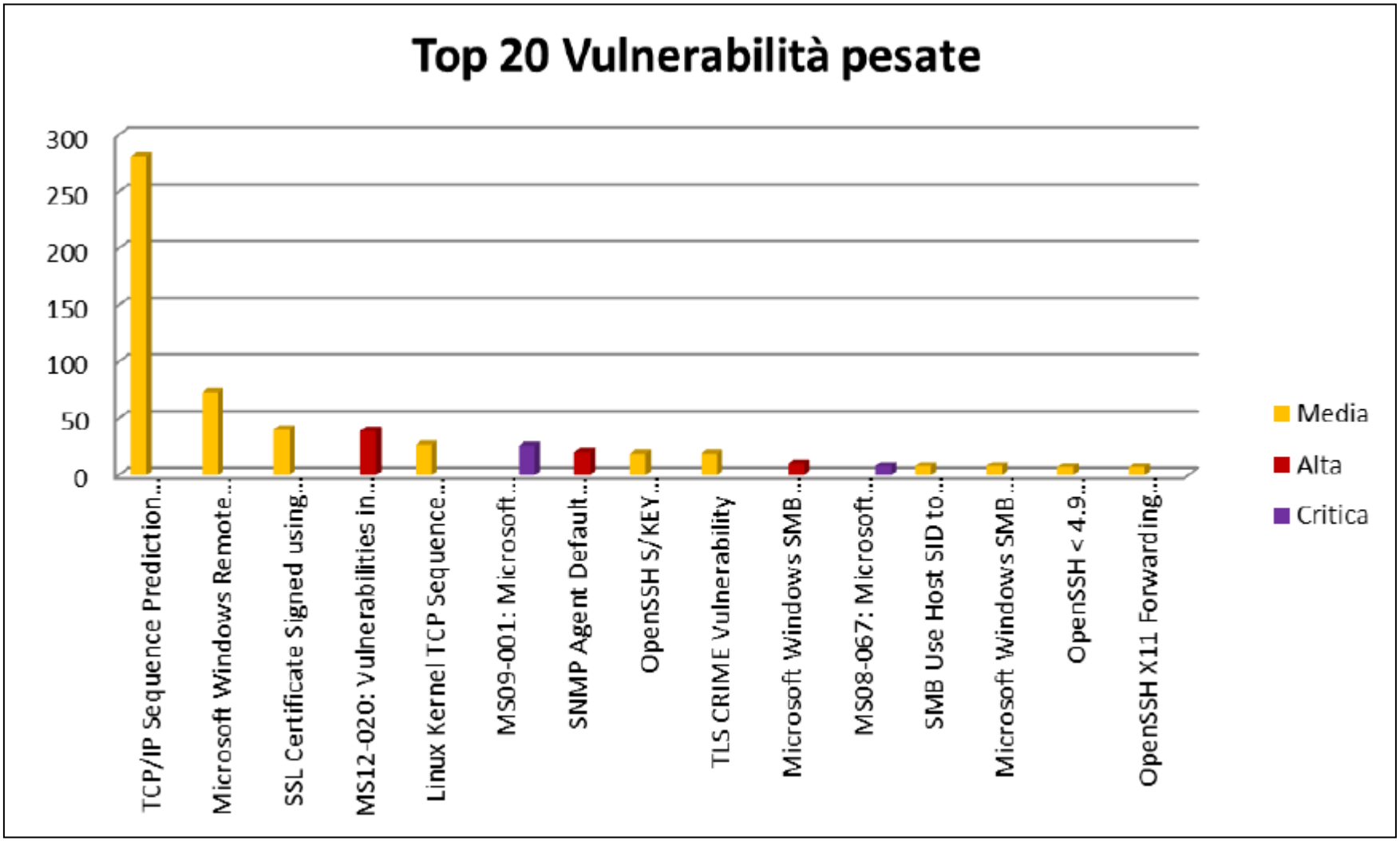
- **Anomalia**: il sistema risponde in modo non consono agli standard
- **Bassa**: un servizio o informazione esposto può essere oggetto di attacco informatico, tuttavia non contiene lacune o vulnerabilità
- **Media**: esiste un potenziali pericolo, ma difficilmente sfruttabile
- **Alta**: il sistema è vulnerabile ed espone informazioni sensibili. Ad esempio un sistema non aggiornato o una pagina Web che espone informazioni aziendali o di sistema
- **Critica** : il sistema permette accessi in lettura/scrittura non autorizzati. E’ possibile modificare lo stato del sistema

Report

- Istogrammi delle vulnerabilità
  - Distribuzione per gravità
  - Top 20 host per vulnerabilità
  - Top 20 vulnerabilità pesate
  - Elenco delle vulnerabilità più critiche con host affetti

- Inquadramento dei risultati in ottica ISO 27001


Distribuzione Vulnerabilità
9%
31%
60%
Media
Alta
Critica


Top 20 Vulnerabilità pesate
300
250
200
150
100
50
0
TCP/IP Sequence Prediction...
Microsoft Windows Remote...
SSL Certificate Signed using...
MS12-020: Vulnerabilities in...
Linux Kernel TCP Sequence...
MS09-001: Microsoft...
SNMP Agent Default...
OpenSSH S/KEY...
TLS CRIME Vulnerability
Microsoft Windows SMB...
MS08-067: Microsoft...
SMB Use Host SID to...
Microsoft Windows SMB...
OpenSSH < 4.9...
OpenSSH X11 Forwarding...
Media
Alta
Critica

Report

- rilevazione di Reti wireless
  - L’analisi è stata effettuata allo scopo di individuare eventuali access point non autorizzati e connessi alla rete del Comune di Vicenza. Non ne sono stati rilevati
- Non rilevato traffico anomalo causato da virus
- Risultati pc estraneo inserito in rete
  - Accesso alle cartelle non protette ,accesso DNS, elenco account

Soluzioni

- Vulnerabilità critiche subito affrontate e risolte
  - Esempio: aggiornamento dei sistemi operativi sui PC tramite policy su Active Directory, impostato il WSUS come server interno per Windows Update
- Soluzioni pianificate
  - Aggiornamenti dei sistemi operativi dei server, per evitare interruzione del servizio

- Implementati con risorse interne al Comune

Soluzioni

- Policy sulle password di Windows e posta elettronica
  - Attivato il blocco degli account dopo *N* tentativi falliti
  - complessità e scadenza della password ogni 3 mesi
  - sostituito password non banali, ove rilevate
- Chiusura cartelle condivise trovate su PC

Soluzioni

- Disattivato Zone Transfer del DNS
  - poteva permettere a utenti non autenticati di scaricare l’intero db con i nomi degli host della rete

Progetti

- Programmi di formazione all’utente
- integrare il regolamento informatico con punti relativi ai dispositivi portartili (pc smathphone e tablet) nell’uso fuori dalla rete comunale , uso wifi
- Sistemi e procedure di monitoraggio continuo