Mail SPF, DKIM, DMARC

Answers

- has opportunistic encryption being used?
  - Answer: Compass to HSR (not sure though... but it seems to me that am encrypted connection was used to send the mail but CA could not be verified)
- is the smtp communication using spf protection?
  - yes.. see excel
- is the smtp communication using dkim protection?
  - yes.. (see mail headers and server logs.) Also see excel
- is the smtp communication using dmarc protection?
  - generally yes (except Compass to HSR where I didn't find any info)

Checks

CHECK SPS

1. Check if sender has SPS info
   - e.g.: `dig -t txt hsr.ch +noall +answer` (hsr.ch is domain from from email)
     - answer with SPF: "v=spf1 mx a:sismtp01.ost.ch ip6:2001:620:130:a036::18 ip6:2001:620:130:a036::19 ip4:152.96.21.228 ip4:152.96.21.229 ip4:152.96.36.18 ip4:152.96.36.19 -all"
       - this does just mean that in this example: hsr provides the info for the receiveer to check SPF. It is still up to the receiver to check.
2. Check mail header for X-Spamd-Result: it seems here the checks are visible.

CHECK DKIM

1. In mail header look for DKIM-Signature. Look for s entry (Example: "s=hsr119). -> see text or via https://mha.azurewebsites.net/
2. dig query: `dig +short hsr1119._domainkey.hsr.ch txt`
   - alternativly use DKIM loop via https://mxtoolbox.com/SuperTool.aspx (e.g.: "hsr.ch:hsr1119")
3. With DKIM-Signature in mail and (public) key in DNS entry, it is possible to verify email
4. Check if DKIM-Signature was verified:
   - see server logs of receiver
   - see mail header X-Spamd-Result

CHECK DMARC

1. Check if there is a DNS entry:
   - `dig -t txt _dmarc.hsr.ch +short` (hsr.ch has no DMARC entry)
   - Alternativly: https://mxtoolbox.com/DMARC.aspx
     https://mxtoolbox.com
2. Check mail header for X-Spamd-Result: it seems here the checks are visible. (probably relevant here)

Notes

- **HSR to compass (1 mail)**
  - Outlook msg -> see png or header.txt (no need to check *.msg file https://emailheaders.net/outlook.html)
  - Mail + Header: https://mha.azurewebsites.net/
    - hsr to compass
  - Traffic (Wireshark *.pcap file)
    - encrypted: Server certificate from HSR
      - 152.96.36.18 mx1.hsr.ch
      - mx1.compass-security.com
  - logs
    - DKIM successful Findings:
- HSR has no DMARC entry -> DNS query via https://mxtoolbox.com/DMARC.aspx¨
- HSR has SPF entry (dig -t txt hsr.ch or also via mxtoolbox.com) and 152.96.36.19 is allowed to send
  - I don't see this verified in the logs, so I guess compass doesn't have SPF checks
- HSR has DKIM which was used here

Hacking-Lab to Compass

- DKIM used and verified
- Hacking-lab has DMARC and SPF entry
  - but i cannot see SPF entry verified in logs (and if no checks fails, DMARC is not relevant)
- from my understanding, the connection between hacking-lab and compass was not encrypted, but the compass receiving server would forward the mail via TLS to another internal mail server.

gmail to Compass gmail has: SPF, DKIM and DMARC entries.

- DKIM check was successful according to logs

compass to hsr We only got the logs of the sender. SPF pass visible in log.

Generally Mail header: each mail server usually adds information to the header. Usually adds "Received" (and other stuff). Existing headers, are usually not changed, but can be over/rewritten (X-Envelope...). https://serverfault.com/questions/163160/when-an-email-is-forwarded-does-it-lose-its-original-headers