

External Network Vulnerability Assessment Report

Project / Client:

Sample Company s.r.o.

Target Resources:

sample-company.sk, www.sample-company.sk, 203.0.113.10

Assessment Type:

External Network Vulnerability Assessment

Date of Assessment:

Sample date range

Prepared By:

ChronosSec | Senior Cybersecurity Engineer

Document Version:

Sample 1.0

Important Sample Note

This is a public sample report. All client names, domains, IP addresses and evidence are synthetic and use reserved example ranges. The design follows the internal ChronosSec report format.

Contents

1. Executive Summary	3
2. Scope & Methodology	3
3. Summary of Findings	4
4. Detailed Findings	5
4.1. Publicly Exposed Database Service	5
4.2. Public FTP Service Exposed	6
4.3. Publicly Exposed Auxiliary HTTP Service on TCP/8888	7
4.4. DMARC Policy Set to Monitoring Mode Only	8
4.5. Missing HTTP Security Headers Including HSTS	9
4.6. Diagnostic Header Disclosure	10
4.7. Legacy CBC TLS Cipher Suites Offered	10
4.8. TLS Certificate Expiring in Less Than 30 Days	11
4.9. OCSP Stapling Not Offered	12
4.10. Mail Authentication Allowed Before TLS	13
5. Positive Security Observations	16
6. Conclusion	17
Appendix A. Key Collected Evidence	18

1. Executive Summary

This sample report presents the results of an external, black-box, non-intrusive network vulnerability assessment conducted against public-facing assets associated with a fictional SMB organization. The assessment focuses on identifying externally reachable services, public DNS and email-security posture, HTTP/TLS configuration, and observable exposure risks without destructive testing, credential attacks, exploitation, or authenticated access attempts.

The sample assessment identified several externally reachable services on the public IP address used by the primary website, including FTP, HTTP/HTTPS, a database service, and an auxiliary HTTP service on TCP/8888. The most significant exposure is the publicly accessible database service on TCP/3306, which reveals service information and should be urgently reviewed and restricted if not explicitly required for public access.

A second high-risk issue was identified on public mail services. SMTP, IMAP, and POP3 services allow plaintext authentication mechanisms to be initiated before TLS negotiation. This may expose credentials if users rely on misconfigured, legacy, or non-strict mail clients.

The website TLS configuration is generally strong: obsolete protocol versions are not offered, while TLS 1.2 and TLS 1.3 are available. However, hardening opportunities were identified, including enabling HSTS, removing legacy CBC cipher suites where possible, removing unnecessary diagnostic headers, and implementing common HTTP security headers.

Email domain protection is partially implemented through SPF, but DMARC is configured in monitoring mode only (p=none). This does not instruct receiving mail servers to quarantine or reject spoofed messages and should be moved toward enforcement after validation.

Overall Risk Level: HIGH

2. Scope & Methodology

Scope of Testing:

- Primary domain: sample-company.sk
- Web alias: www.sample-company.sk
- Resolved public IP observed during the sample assessment: 203.0.113.10
- Mail host observed during the sample assessment: mail.sample-company.sk / 198.51.100.25
- Testing was limited to non-intrusive external validation and did not include exploitation, brute-force attacks, password spraying, denial-of-service testing, web fuzzing, or authenticated access.

Methodology:

- Passive DNS, WHOIS, MX, SPF, DMARC and name-server review.
- Low-rate TCP service discovery and service fingerprinting against confirmed public assets.
- HTTP/HTTPS header review and TLS validation using standard command-line tools.
- Safe DNS zone transfer validation against authoritative name servers.
- Manual review of collected evidence and risk classification based on externally observable exposure.

Tools Utilized:

- dig
- whois
- curl
- openssl
- nmap

- testssl.sh
- netcat

Limitations:

- The assessment did not verify credentials, attempt logins, exploit vulnerabilities, or perform intrusive application testing.
- All evidence in this report is synthetic and intended for public sample use only.
- Findings are based on externally observable evidence collected during a sample assessment window.

3. Summary of Findings

Risk Level	Count	Impact Description	Related Findings
High	2	Requires urgent review. Publicly reachable database services and insecure authentication flows expose sensitive attack surface and should normally not be accessible from the Internet.	EXT-001, EXT-010
Medium	4	Externally reachable services and configuration weaknesses that increase exposure, phishing/spoofing risk, or weaken browser-side protection.	EXT-002, EXT-003, EXT-004, EXT-005
Low	2	Hardening weaknesses and information disclosure that do not directly prove compromise but should be remediated.	EXT-006, EXT-007
Informational	2	Operational observations that should be monitored or reviewed as part of routine service hardening.	EXT-008, EXT-009

ID	Finding	Severity	Affected Asset	Status
EXT-001	Publicly Exposed Database Service	High	203.0.113.10:3306	Confirmed
EXT-002	Public FTP Service Exposed	Medium	203.0.113.10:21	Confirmed
EXT-003	Externally Accessible HTTP Service on TCP/8888	Medium	203.0.113.10:8888	Confirmed
EXT-004	DMARC Policy Set to Monitoring Mode Only	Medium	sample-company.sk	Confirmed
EXT-005	Missing HTTP Security Headers Including HSTS	Medium	sample-company.sk	Confirmed
EXT-006	Diagnostic Header Disclosure	Low	sample-company.sk	Confirmed
EXT-007	Legacy CBC TLS Cipher Suites Offered	Low	sample-company.sk:443	Confirmed
EXT-008	TLS Certificate Expiring in Less Than 30 Days	Informational	sample-company.sk:443	Confirmed
EXT-009	OCSP Stapling Not Offered	Informational	sample-company.sk:443	Confirmed
EXT-010	Mail Authentication Allowed Before TLS	High	mail.sample-company.sk / 198.51.100.25	Confirmed

4. Detailed Findings

4.1. Publicly Exposed Database Service

Risk Level:	High
Affected Asset:	203.0.113.10
Affected Port(s):	3306/tcp
Status:	Confirmed (sample evidence)

Description:

A database service was identified as externally reachable on TCP/3306. The service exposes version information and supports password-based authentication. Public exposure of database services significantly increases the attack surface and may enable credential attacks, service fingerprinting, and exploitation if a relevant vulnerability or weak credential exists.

Proof of Concept / Evidence:

```
$ nmap -Pn -T2 -sV -p 3306 --script mysql-info 203.0.113.10
PORT STATE SERVICE VERSION
3306/tcp open  mysql MariaDB 10.x
mysql-info:
  Protocol: 10
  Version: 10.x-MariaDB
  Auth Plugin Name: mysql_native_password
Nmap done: 1 IP address (1 host up) scanned.
```

Impact:

Database services should not normally be exposed directly to the public Internet. Even where authentication is required, public exposure allows unauthenticated fingerprinting and increases the likelihood of password attacks, vulnerability targeting, and accidental data-layer exposure.

Remediation:

- Restrict TCP/3306 from the public Internet.
- Allow database access only from trusted internal application servers, VPN, or administrative IP ranges.
- If remote database access is required, enforce strict source IP allowlisting and TLS.
- Confirm whether the exposed database service belongs to the client or to the hosting provider.
- Review authentication settings and enforce strong, unique credentials.

4.2. Public FTP Service Exposed

Risk Level:	Medium
Affected Asset:	203.0.113.10
Affected Port(s):	21/tcp
Status:	Confirmed (sample evidence)

Description:

An FTP service was identified as externally reachable on TCP/21. Plain FTP may transmit credentials and data without encryption unless FTPS is enforced. Public FTP exposure also increases the risk of credential attacks and service-specific vulnerability exposure.

Proof of Concept / Evidence:

```
$ nc -v 203.0.113.10 21
Connection to 203.0.113.10 21 port [tcp/ftp] succeeded!
220 203.0.113.10 FTP server ready
221 Goodbye.

$ nmap -Pn -T2 -sV -p 21,80,443,3306,8888 203.0.113.10
21/tcp open  ftp ProFTPD
80/tcp open  http nginx
443/tcp open ssl/http nginx
3306/tcp open mysql MariaDB
8888/tcp open http nginx
```

Impact:

If FTP is used for administrative content uploads, credential compromise may lead to website modification or unauthorized file access. If the service supports only plaintext FTP, credentials could be exposed on untrusted networks.

Remediation:

- Disable FTP if it is not required.
- Prefer SFTP or FTPS for administrative file transfer.
- Restrict access to approved source IP addresses only.
- Disable anonymous FTP access and enforce strong credentials.
- Keep FTP software updated and monitor authentication logs.

4.3. Publicly Exposed Auxiliary HTTP Service on TCP/8888

Risk Level:	Medium
Affected Asset:	203.0.113.10
Affected Port(s):	8888/tcp
Status:	Confirmed (sample evidence)

Description:

An externally accessible HTTP service was identified on non-standard TCP port 8888. The service returns a status message to unauthenticated users. While no administrative interface was identified during the non-intrusive review, the service appears to expose hosting or security-related functionality and should be reviewed for business necessity, ownership, and access restrictions.

Proof of Concept / Evidence:

```
$ nmap -Pn -T2 -sV -p 8888 --version-light 203.0.113.10
PORT STATE SERVICE VERSION
8888/tcp open  http nginx

$ curl -I http://sample-company.sk:8888/
HTTP/1.1 200 OK
Server: nginx
Content-Type: text/plain; charset=UTF-8
X-Content-Type-Options: nosniff

$ curl -s http://sample-company.sk:8888/
Your IP 198.51.100.200 is not blocked
```

Impact:

Publicly exposed auxiliary services on non-standard ports may increase the external attack surface and reveal operational information about hosting or access-control mechanisms. If this service is administrative, provider-related, or not required for public users, it should not be exposed to the Internet.

Remediation:

- Confirm whether TCP/8888 is required for the client website or belongs to the hosting provider.
- If not required, disable the service or restrict access by source IP.
- If required for administrative or support purposes, place it behind VPN or provider-side access controls.
- Avoid exposing operational status messages to unauthenticated Internet users.
- Use HTTPS if the service must remain externally reachable.

4.4. DMARC Policy Set to Monitoring Mode Only

Risk Level:	Medium
Affected Asset:	sample-company.sk
Affected Port(s):	DNS TXT / _dmarc
Status:	Confirmed (sample evidence)

Description:

The domain has a DMARC record, but the policy is set to p=none. This provides monitoring only and does not instruct receiving mail servers to quarantine or reject spoofed messages that fail authentication.

Proof of Concept / Evidence:

```
$ dig +short TXT _dmarc.sample-company.sk
"v=DMARC1; p=none; rua=mailto:dmarc@sample-company.sk"

$ dig +short TXT sample-company.sk
"v=spf1 a mx include:_spf.example-mail.invalid -all"

$ dig +short MX sample-company.sk
10 mail.sample-company.sk.
```

Impact:

A monitoring-only DMARC policy may allow spoofed messages using the organization domain to be delivered if SPF/DKIM alignment fails. For an SMB organization, this can increase exposure to invoice fraud, supplier impersonation, business email compromise, and phishing.

Remediation:

- Validate legitimate mail flows and collect DMARC aggregate reports.
- Move gradually from p=none to p=quarantine and then p=reject.
- Ensure SPF and DKIM alignment for all authorized mail sources.
- Monitor rejected and quarantined messages after enforcement.

4.5. Missing HTTP Security Headers Including HSTS

Risk Level:	Medium
Affected Asset:	sample-company.sk, www.sample-company.sk
Affected Port(s):	80/tcp, 443/tcp
Status:	Confirmed (sample evidence)

Description:

The public website does not return several common HTTP security headers, including Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, Referrer-Policy, and Permissions-Policy. Although HTTP redirects to HTTPS, the absence of HSTS means browsers are not explicitly instructed to always use HTTPS for future connections.

Proof of Concept / Evidence:

```
$ curl -I http://sample-company.sk/
HTTP/1.1 301 Moved Permanently
Server: nginx
Location: https://sample-company.sk/

$ curl -I https://sample-company.sk/
HTTP/2 200
server: nginx
content-type: text/html
x-vhost-debug: sample-routing-id
# Strict-Transport-Security: not observed
# Content-Security-Policy: not observed
# X-Frame-Options: not observed
```

Impact:

Missing security headers may increase exposure to downgrade-related risks, clickjacking, MIME sniffing, browser feature abuse, and content-injection impact if a separate web vulnerability is present.

Remediation:

- Enable HSTS after confirming HTTPS works correctly across all required subdomains.
- Add X-Content-Type-Options: nosniff.
- Add X-Frame-Options: SAMEORIGIN or a CSP frame-ancestors directive.
- Add Referrer-Policy: strict-origin-when-cross-origin.
- Add a carefully tested Content-Security-Policy suited to the site resources.
- Add Permissions-Policy to disable unnecessary browser features.

4.6. Diagnostic Header Disclosure

Risk Level:	Low
Affected Asset:	sample-company.sk, www.sample-company.sk
Affected Port(s):	80/tcp, 443/tcp
Status:	Confirmed (sample evidence)

Description:

The web server returns a diagnostic header in public HTTP responses. While this does not directly expose sensitive data, debug or internal routing headers should generally not be disclosed to unauthenticated Internet users.

Proof of Concept / Evidence:

```
$ curl -sI https://sample-company.sk/  
HTTP/2 200  
server: nginx  
date: Sample-Date  
content-type: text/html  
x-vhost-debug: sample-routing-id  
cache-control: public, max-age=3600
```

Impact:

Unnecessary diagnostic headers can disclose implementation or hosting-layer information and may help attackers fingerprint routing behavior or virtual-host configuration.

Remediation:

- Remove diagnostic and debug headers from public responses.
- Review web server and hosting provider configuration for debug header exposure.
- Maintain only headers required for normal browser and proxy behavior.

4.7. Legacy CBC TLS Cipher Suites Offered

Risk Level:	Low
Affected Asset:	sample-company.sk
Affected Port(s):	443/tcp
Status:	Confirmed (sample evidence)

Description:

The TLS service offers CBC-based cipher suites under TLS 1.2. Modern AEAD cipher suites and TLS 1.3 are supported, and the overall TLS posture is strong, but CBC ciphers may expose legacy clients to known cryptographic weaknesses such as Lucky13-style attacks.

Proof of Concept / Evidence:

```
$ testssl.sh --warnings batch https://sample-company.sk/  
TLS 1.3 offered (OK)  
TLS 1.2 offered (OK)  
TLS 1.1 not offered (OK)  
TLS 1.0 not offered (OK)  
SSLv3 not offered (OK)  
Obsolete CBC ciphers: offered  
Overall grade: A
```

Impact:

This is primarily a hardening issue because modern protocols and forward-secret AEAD cipher suites are available. However, disabling CBC cipher suites reduces legacy cryptographic exposure and improves the TLS baseline.

Remediation:

- Prefer TLS 1.3 and TLS 1.2 AEAD cipher suites only.
- Disable CBC-based TLS 1.2 cipher suites where compatibility requirements allow.
- Keep ECDHE + AES-GCM and CHACHA20-POLY1305 suites enabled.
- Re-test after changes to confirm compatibility for expected users.

4.8. TLS Certificate Expiring in Less Than 30 Days

Risk Level:	Informational
Affected Asset:	sample-company.sk, www.sample-company.sk
Affected Port(s):	443/tcp
Status:	Confirmed (sample evidence)

Description:

The HTTPS certificate is valid and trusted, but it was observed to expire within less than 30 days from the sample assessment date. This is common for short-lived certificates but should be monitored to ensure automated renewal works correctly.

Proof of Concept / Evidence:

```
$ echo | openssl s_client -connect sample-company.sk:443 -servername sample-company.sk 2>/dev/null | openssl x
509 -noout -issuer -subject -dates -ext subjectAltName
issuer=C = US, O = Example CA, CN = Example R3
subject=CN = sample-company.sk
notBefore=Sample-Date
notAfter=Sample-Date+27days
X509v3 Subject Alternative Name:
DNS:sample-company.sk, DNS:www.sample-company.sk
```

Impact:

If automated renewal fails, users may receive certificate warnings and the website may become inaccessible or distrusted. This is an operational monitoring issue rather than an immediate security failure.

Remediation:

- Confirm automated certificate renewal is enabled and functioning.
- Monitor certificate expiry and alert before renewal failure.
- Verify renewal also covers both sample-company.sk and www.sample-company.sk.

4.9. OCSP Stapling Not Offered

Risk Level:	Informational
Affected Asset:	sample-company.sk
Affected Port(s):	443/tcp
Status:	Confirmed (sample evidence)

Description:

The HTTPS service does not offer OCSP stapling. This does not directly indicate compromise, but enabling OCSP stapling can improve certificate status validation performance and privacy for clients.

Proof of Concept / Evidence:

```
$ testssl.sh --warnings batch https://sample-company.sk/ | grep -Ei "OCSP URI|OCSP stapling|OCSP must staple"
OCSP URI --
OCSP stapling not offered
OCSP must staple extension --
```

Impact:

Without OCSP stapling, clients may need to validate certificate revocation status independently where supported. This may slightly reduce performance and privacy compared to stapled responses.

Remediation:

- Enable OCSP stapling where supported by the hosting platform and certificate chain.
- Validate that stapled responses are fresh and correctly served after enabling.
- Treat this as secondary hardening after remediating exposed database and FTP services.

4.10. Mail Authentication Allowed Before TLS

Risk Level:	High
Affected Asset:	mail.sample-company.sk / 198.51.100.25
Affected Port(s):	25/tcp, 587/tcp, 110/tcp, 143/tcp
Status:	Confirmed (sample evidence)

Description:

The public mail services allow authentication mechanisms to be initiated before an encrypted TLS session is established. SMTP services on ports 25 and 587 advertise AUTH LOGIN and AUTH PLAIN before STARTTLS is negotiated. IMAP on port 143 advertises AUTH=PLAIN and AUTH=LOGIN before STARTTLS. POP3 on port 110 advertises USER and SASL PLAIN/LOGIN before STLS.

Proof of Concept / Evidence:

```
$ nc -v mail.sample-company.sk 587
mail.sample-company.sk [198.51.100.25] 587 (submission) open
220 mail.sample-company.sk ESMTP
250-AUTH LOGIN PLAIN
250-STARTTLS
334 VXNlcm5hbWU6
501 Authentication cancelled

$ nc -v mail.sample-company.sk 143
* OK [CAPABILITY IMAP4rev1 STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
+
a002 BAD Authentication aborted by client.

$ nc -v mail.sample-company.sk 110
+OK Dovecot ready.
CAPA
STLS
USER
SASL PLAIN LOGIN
.
```

Impact:

An attacker with the ability to observe or manipulate network traffic between the user and the mail server could potentially capture mail credentials if authentication is performed before TLS is established. Successful credential compromise could allow mailbox access, phishing, invoice fraud, password resets, forwarding-rule persistence, and access to sensitive business communications.

Remediation:

- Do not advertise AUTH LOGIN/PLAIN before STARTTLS.
- Allow AUTH only after STARTTLS on ports 25/587 or only on implicit TLS port 465.
- Disable AUTH=PLAIN and AUTH=LOGIN on port 143 before STARTTLS.
- Enable LOGINDISABLED until STARTTLS is negotiated.
- Disable USER/PASS and SASL PLAIN/LOGIN on port 110 before STLS.
- Prefer POP3S on port 995 only.
- Configure mail clients to require encrypted connections and reject certificate validation errors.

5. Positive Security Observations

- HTTP redirects to HTTPS using a 301 response.
- SSLv2 and SSLv3 are not offered.
- TLS 1.0 and TLS 1.1 are not offered.
- TLS 1.2 and TLS 1.3 are supported.
- Forward secrecy is offered.
- The certificate chain is valid and trusted.
- SPF is configured with a hard fail policy (-all).
- DNS zone transfer was tested against authoritative name servers and was not permitted.
- No public administrative login page was identified on TCP/8888 during the limited non-intrusive check.

DNS AXFR validation:

```
==== ns1.example-dns.invalid ====
$ dig @ns1.example-dns.invalid sample-company.sk AXFR
; Transfer failed.

==== ns2.example-dns.invalid ====
$ dig @ns2.example-dns.invalid sample-company.sk AXFR
; Transfer failed.
```

6. Conclusion

The external non-intrusive assessment identified a concentrated set of externally reachable services on the public IP address used by the sample company website. The most important risk is the public exposure of the database service on TCP/3306. This should be treated as the first remediation priority because database services should normally be isolated from direct Internet reachability.

The second priority is to review and restrict the public FTP service and the auxiliary HTTP service on TCP/8888. These services may belong to a hosting provider or shared hosting environment; therefore, ownership and business necessity should be confirmed before remediation planning. If they are not required for public access, they should be disabled or restricted through firewall rules, VPN, or source-IP allowlisting.

The public website TLS configuration is generally strong, with obsolete protocol versions disabled and TLS 1.3 available. Remaining web hardening tasks include enabling HSTS, adding common security headers, removing diagnostic headers, and disabling legacy CBC cipher suites where compatibility allows.

Email domain protection should be improved by moving DMARC from monitoring mode toward quarantine and eventually reject after validating legitimate mail flows. Together, these actions would materially reduce the organization's public attack surface, improve browser-side protection, and strengthen resistance to email spoofing and business email compromise.

Mail services should also be reviewed urgently because SMTP, IMAP and POP3 authentication mechanisms are available before TLS negotiation, creating a potential plaintext credential exposure scenario for misconfigured or legacy clients.

Appendix A. Key Collected Evidence

WHOIS / Registrar:

Registrar: Example Registrar, a.s.

Technical organisation: Example Registrar, a.s.

Name servers: ns1.example-dns.invalid, ns2.example-dns.invalid

DNS records:

sample-company.sk A 203.0.113.10

www.sample-company.sk A 203.0.113.10

MX record: mail.sample-company.sk

Confirmed open services:

21/tcp open ftp ProFTPD

80/tcp open http nginx

443/tcp open ssl/http nginx

3306/tcp open mysql MariaDB

8888/tcp open http nginx

TLS summary:

SSLv2: not offered

SSLv3: not offered

TLS 1.0: not offered

TLS 1.1: not offered

TLS 1.2: offered

TLS 1.3: offered

Overall Grade: A

Mail host:

mail.sample-company.sk A 198.51.100.25

25/tcp open smtp

465/tcp open ssl/smtp

587/tcp open smtp

110/tcp open pop3

143/tcp open imap

993/tcp open ssl/imap

995/tcp open ssl/pop3

Observed issue: AUTH LOGIN/PLAIN advertised before STARTTLS/STLS on plaintext mail ports.