CYBER-ESSENTIALS-BERICHT

Example GmbH

ZEITRAUM	DOMAINS	HOSTS	ERSTELLT AM
23.6.2026 – 21.9.2026	1	8	14.10.2026

Dieser Bericht ordnet die von außen erkennbaren Befunde von Example GmbH den fünf technischen Kontrollen von Cyber Essentials zu, dem Zertifizierungsprogramm des britischen NCSC (Anforderungen v3.3, Fragenkatalog „Danzell“, gültig seit 27. April 2026). Er zeigt, wo extern schon Handlungsbedarf erkennbar ist und was Sie intern noch nachweisen müssen. veyrisk zertifiziert nicht.

1. Überblick

4 offene Befunde sprechen voraussichtlich gegen ein Bestehen. Beheben Sie diese vor der Selbstauskunft.

KONTROLLE	STAND	OFFENE BEFUNDE	VORAUSSICHTLICH NICHT BESTANDEN
Firewalls	BEFUNDE OFFEN	3	2
Sichere Konfiguration	BEFUNDE OFFEN	5	0
Management von Sicherheitsupdates	BEFUNDE OFFEN	1	1
Benutzerzugriffskontrolle	BEFUNDE OFFEN	1	1
Schutz vor Schadsoftware	VON AUSSEN NICHT PRÜFBAR	0	0

2. Firewalls

BEFUNDE OFFEN

Was veyrisk von außen prüft

Aus dem Internet dürfen nur benötigte Dienste erreichbar sein. veyrisk prüft offene Ports (nur mit Besitznachweis), öffentlich erreichbare Verwaltungsoberflächen sowie Entwicklungs- und Testsysteme.

SCHWEREGRAD	BEFUND	OFFEN SEIT (TAGEN)	HINWEIS

HOCH	vpn.example.com RDP aus dem Internet erreichbar (Port 3389)	38	HOCH ODER KRITISCH UND LÄNGER ALS 14 TAGE OFFEN
HOCH	shop.example.com Verwaltungsoberfläche öffentlich erreichbar (phpMyAdmin)	61	HOCH ODER KRITISCH UND LÄNGER ALS 14 TAGE OFFEN
MITTEL	dev.example.com Entwicklungs- oder Testsystem öffentlich erreichbar	61	

Intern nachzuweisen

- Firewall an jeder Grenze zum Internet, Standardpasswort der Firewall geändert
- Jede eingehende Freigabe dokumentiert und begründet, nicht mehr benötigte Regeln entfernt
- Software-Firewall auf Geräten, die in fremden Netzen wie WLAN-Hotspots genutzt werden

3. Sichere Konfiguration

BEFUNDE OFFEN

Was veyrisk von außen prüft

Geräte und Dienste sind gehärtet: keine unnötige Software, keine Standardkonten, sichere Voreinstellungen. veyrisk prüft Zertifikate, TLS, HTTPS, Sicherheits-Header und Versionsangaben sowie Konfigurationsbefunde aus Web-App- und Cloud-Prüfungen.

SCHWEREGRAD	BEFUND	OFFEN SEIT (TAGEN)	HINWEIS
MITTEL	mail.example.com TLS-Zertifikat läuft in 9 Tagen ab	3	
MITTEL	shop.example.com HSTS-Header fehlt	90	
NIEDRIG	www.example.com Softwareversion im Header Server sichtbar (Apache/2.4.49)	45	
NIEDRIG	www.example.com Content-Security-Policy fehlt	90	
NIEDRIG	portal.example.com X-Content-Type-Options fehlt	90	

Intern nachzuweisen

- Nicht benötigte Software, Dienste und Benutzerkonten entfernt oder deaktiviert
- Standardpasswörter geändert, automatisches Ausführen (Autorun) deaktiviert
- Gerätesperre per PIN, Passwort oder Biometrie auf allen Geräten

4. Management von Sicherheitsupdates

BEFUNDE OFFEN

Was veyrisk von außen prüft

Alle Software ist lizenziert und wird vom Hersteller noch unterstützt. Kritische und hochriskante Updates müssen innerhalb von 14 Tagen nach Erscheinen installiert sein. veyrisk nutzt dafür die Befunde aus Advanced Vulnerability Detection und Web-App-Befunde mit CVE.

SCHWEREGRAD	BEFUND	OFFEN SEIT (TAGEN)	HINWEIS
HOCH	vpn.example.com OpenSSH 'regreSSHion' Remote Code Execution Vulnerability (22/tcp)	26	HOCH ODER KRITISCH UND LÄNGER ALS 14 TAGE OFFEN

Intern nachzuweisen

- Inventar aller Geräte im Geltungsbereich mit Betriebssystem und Version
- Nur unterstützte Betriebssysteme und Anwendungen im Einsatz, nicht mehr unterstützte entfernt oder abgetrennt
- Automatische Updates eingeschaltet, wo möglich, sonst Nachweis der Installation innerhalb von 14 Tagen

5. Benutzerzugriffskontrolle

BEFUNDE OFFEN

Was veyrisk von außen prüft

Konten gibt es nur nach Bedarf, Administratorrechte werden getrennt genutzt. MFA ist auf allen Cloud-Diensten Pflicht, die sie anbieten; fehlt sie, gilt die Prüfung automatisch als nicht bestanden. Passkeys zählen als passwortlose Anmeldung. veyrisk sieht das nur in verbundenen Cloud- und Microsoft-365-Konten.

SCHWEREGRAD	BEFUND	OFFEN SEIT (TAGEN)	HINWEIS

HOCH	Microsoft 365 (example.com) Ensure multifactor authentication is enabled for all users	9	MFA FEHLT: FÜHRT AUTOMATISCH ZUM NICHTBESTEHEN

Intern nachzuweisen

- MFA auf allen Cloud-Diensten, die sie anbieten, für alle Benutzer
- Getrennte Administratorkonten, die nicht für E-Mail und Surfen genutzt werden
- Geregelter Ablauf zum Anlegen und Entfernen von Konten, regelmäßige Überprüfung der Rechte
- Passwortregeln oder passwortlose Anmeldung mit Passkeys, Schutz gegen Rateangriffe

6. Schutz vor Schadsoftware

VON AUSSEN NICHT PRÜFBAR

Was veyrisk von außen prüft

Auf allen Geräten im Geltungsbereich läuft ein Schutz vor Schadsoftware. Das lässt sich von außen nicht prüfen.

Schutz vor Schadsoftware lässt sich von außen nicht prüfen.

Intern nachzuweisen

- Virenschutz mit aktuellen Signaturen auf allen Geräten oder Freigabeliste für Anwendungen (Application Allow-Listing)
- Prüfung von Dateien beim Zugriff und Schutz vor schädlichen Websites

7. Hinweise und Grenzen

Dieser Bericht ist ein Readiness-Check von außen und keine Zertifizierung. veyrisk zertifiziert nicht. Cyber Essentials und Cyber Essentials Plus vergeben ausschließlich von IASME lizenzierte Zertifizierungsstellen; Cyber Essentials Plus ergänzt eine technische Prüfung. Das Zertifikat gilt 12 Monate.

Zum Geltungsbereich gehören alle Geräte mit Internetverbindung und alle Cloud-Dienste. veyrisk sieht davon nur die öffentlich erreichbaren Systeme Ihrer Domains und verbundene Cloud-Konten. Schutz vor Schadsoftware und der größte Teil der Zugriffskontrolle lassen sich von außen nicht prüfen.

Die Zuordnung der Befunde zu den Kontrollen ist eine Einschätzung von veyrisk. Befunde zur E-Mail-Authentisierung (SPF, DMARC, MTA-STS) gehören zu keiner der fünf Kontrollen und erscheinen hier nicht. Maßgeblich sind die Anforderungen des NCSC und die Bewertung Ihrer Zertifizierungsstelle.

VEYRISK · NEONOTU GMBH

Edelsbergstraße 8, 80686 München · +49 89 2000 7975 0 · contact@veyrisk.com