

KI-gestützte Cyberangriffe auf KMU

Schutzmaßnahmen 2026

Nexcraft-Labs · Beratungsunterlage · Wien, 14. Oktober 2026

Was hat sich verändert?

Früher	Heute mit KI
Phishing: schlechtes Deutsch, generisch	Personalisiert — Firmennamen, Bank, Lieferant
Angriff dauerte Tage bis Wochen	Von Erkundung bis Ausführung unter einer Stunde
Nur erfahrene Angreifer	Keine technischen Kenntnisse mehr nötig
Stimmen und Videos nicht fälschbar	CEO-Fraud per Deepfake-Anruf (Millionenschäden 2024)

Wichtigste Folge: KMU werden nicht mehr übersehen — automatisierte Scans finden jeden offenen Port, jede veraltete CMS-Version und jeden fehlenden DNS-Eintrag.

Maßnahmen — priorisiert nach Wirkung/Aufwand

STUFE 1 — Sofort · geringer Aufwand

- ☐ **E-Mail-Authentifizierung (DMARC + DKIM + SPF)**
*Verhindert, dass Angreifer Ihre Domain für Phishing-Mails missbrauchen.
Fehlt bei über 80 % der österreichischen KMU.*
- ☐ **MFA auf allen wichtigen Zugängen**
*E-Mail, Cloud-Speicher, Banking, Buchhaltungssoftware.
Ein Passwort allein reicht nicht mehr.*
- ☐ **Passwort-Manager einführen (z. B. Bitwarden Teams, ca. 3 €/User/Monat)**
Jeder Dienst bekommt ein eigenes, zufälliges Passwort.

STUFE 2 — Bald · mittlerer Aufwand

- ☐ **Backup-Konzept nach der 3-2-1-Regel**
*3 Kopien · 2 verschiedene Medien · 1 offline.
Ransomware kann nur erpressen, was nicht gesichert ist.*
- ☐ **Patch-Management automatisieren**
*Server und CMS automatisch aktualisieren.
Veraltete Systeme werden in Minuten gefunden.*
- ☐ **Incident-Response-Plan (1 Seite reicht)**
Was tun, wenn es passiert? Wen anrufen? Wie Systeme isolieren?

STUFE 3 — Prozesse · wichtiger als Technik

- ☐ **Rückruf-Regel bei Überweisungen**
*Jede unerwartete Zahlung über 1.000 € → telefonisch bestätigen
über die bekannte Nummer (NICHT die aus der Mail).*
- ☐



Zwei-Kanal-Prinzip bei Dringlichkeit

Zugangsdaten, Freigaben, Geld: immer auf einem zweiten, unabhängigen Kanal bestätigen.

Was Nexcraft-Labs übernimmt

Leistung	Preis	Art
Security-Check (17-Punkte-Audit)	ab 290 €	einmalig
E-Mail-Härtung (DMARC/DKIM/SPF)	ab 190 €	einmalig
MFA + Passwort-Manager-Setup	ab 290 €	einmalig
NIS2-Lieferanten-Nachweis	49 €/Monat	laufend
Security-Care (Patch-Mgmt + Monitoring)	ab 49 €/Monat	laufend

Kostenloser Erstcheck: nexcraft-labs.com/f/ (kein Konto, kein Download, 5 Minuten)

Gerhard Kubik · Nexcraft-Labs

contact@nexcraft-labs.com · +43 650 4955580 · nexcraft-labs.com