Security Baseline für KMU

Die essentiellen Maßnahmen für Ihren digitalen Geschäftserfolg

Einleitung: Warum Sicherheit auch für KMU existenziell ist

Angriffe auf IT-Systeme sind kein Problem, das nur Großkonzerne betrifft. Im Gegenteil: KMU sind aufgrund oft begrenzter Ressourcen und Expertise ein besonders häufiges und lohnendes Ziel für Cyberkriminelle. Die Folgen können verheerend sein: Betriebsstillstand, Datenverlust, Erpressungszahlungen und Reputationsschaden.

Die gute Nachricht: Sie müssen kein Sicherheitskonzern sein, um sich effektiv zu schützen. Mit einem pragmatischen Ansatz, der auf die wesentlichen und umsetzbaren Maßnahmen fokussiert, können Sie Ihr Risiko massiv senken. Diese Baseline ist Ihr erster und wichtigster Werkzeugkasten.

Kapitel 1: Die 3 Säulen der KMU-Sicherheit

Konzentrieren Sie Ihre Kräfte zunächst hierauf. Diese drei Säulen bieten den größten Schutz pro investierter Stunde.

Säule 1: Härtung der Systeme

Die Grundabsicherung Ihrer Technologie.

- Updates & Patches: Alle Betriebssysteme, Anwendungen (v.a. Browser, Office) und Firmware (Router, Firewalls) innerhalb von 14 Tagen nach Veröffentlichung von kritischen Sicherheitsupdates installieren.
- Firewall (lokal): Die eingebaute Firewall auf allen Rechnern ist aktiviert. Eingehende Verbindungen sind standardmäßig blockiert.
- Firewall (Netzwerk): Ihr Internet-Router hat eine aktive Firewall. Unnötige Port-Freigaben (z.B. für Fernzugriff) sind deaktiviert.
- Passwortrichtlinie: Mindestanforderung: 12 Zeichen. Keine Wiederverwendung desselben Passworts für wichtige Dienste (E-Mail, Banking, Admin-Accounts). Nutzen Sie einen Passwortmanager.
- Administratoren-Rechte: Benutzer arbeiten im Alltag nicht mit Admin-Rechten. Ein separates Admin-Konto wird nur bei Bedarf genutzt.
- Unnötige Dienste: Deinstallieren Sie nicht benötigte Software. Schließen Sie nicht genutzte Netzwerkports.

Säule 2: Multi-Faktor-Authentifizierung (MFA)

Die einfachste und effektivste Einzelmaßnahme gegen Account-Übernahmen.

Warum MFA der Game-Changer ist: Ein gestohlenes Passwort reicht nicht mehr aus. Der Angreifer benötigt zusätzlich Ihr Smartphone oder einen Sicherheitsschlüssel.

- Microsoft 365 / Azure AD: Sicherheitsstandards oder Authenticator-App aktivieren.
- Google Workspace: Admin-Konsole > Sicherheit > Authentifizierung > Zweistufige Verifizierung.
- Cloud- & Finanzdienste: AWS, PayPal, Banking, Social-Media-Business-Accounts.
- Methode der Wahl: Authenticator-App statt SMS.

Säule 3: Logging & Monitoring

Sie können nur schützen, was Sie sehen.

- Firewall-Logs: Alle ein- und ausgehenden Verbindungsversuche.
- Admin-Logins: Erfolgreiche und gescheiterte Anmeldeversuche.
- Antivirus / EDR-Logs: Gefundene Malware und Blockierungen.

Kapitel 2: Quick-Win Checkliste

- MFA für alle E-Mail-Adressen aktivieren.
- Kritische Sicherheitsupdates einspielen.
- Passwortmanager einführen.
- Phishing-Schulung durchführen.
- Administrative Rechte entfernen.
- Automatische Bildschirmsperre aktivieren.
- Router-Konfiguration prüfen.
- Backups nach 3-2-1-Regel prüfen.
- Antivirus / EDR aktiv.
- Notfallkontakte bereithalten.
- Unbenutzte Konten deaktivieren.
- WLAN mit Gastnetz absichern.

Kapitel 3: Nächste Schritte & Professionelle Unterstützung

Wenn die Baseline umgesetzt ist, haben Sie bereits 80% des Schutzes mit 20% des Aufwands erreicht.

- Externe Beratung bei Cloud- oder Netzwerkprojekten.
- Erstellung von Sicherheitskonzepten (ISO 27001, TISAX).
- Externe Audits.
- Regelmäßige Penetrationstests.

Dieses Dokument dient als pragmatischer Leitfaden und ersetzt keine individuelle Beratung. Es wird keine Haftung für die Umsetzung übernommen.