Technische Anforderungen an die Infrastruktur und Sicherheit des Partners bei Einführung der Gründerplattform Widgets

1. Infrastruktur Anforderungen

1.1. Regelmäßige Sicherheitspatches & Systemaktualisierungen

- Die Systeme des Partners müssen regelmäßig aktualisiert werden, insbesondere sicherheitsrelevante Komponenten wie:
    - **Betriebssysteme** (z. B. Linux, Windows Server)
    - **Webserver-Software** (z. B. Nginx, Apache, IIS)
    - **Datenbanken** (z. B. MySQL, PostgreSQL, MongoDB)
    - **CMS- und Web-Frameworks** (z. B. WordPress, Laravel, React)
- Kritische Sicherheitspatches müssen innerhalb eines **angemessenen Zeitraums** nach Veröffentlichung installiert werden (empfohlen: innerhalb von 30 Tagen für Hochrisiko-Schwachstellen).
- Automatische Sicherheitsupdates sollten aktiviert sein, sofern dies praktikabel ist.

1.2. Hosting & Netzwerk

- Die Partner-Website oder Webanwendung muss auf einer sicheren Infrastruktur betrieben werden, die Schutz vor **DDoS-Angriffen** und anderen Bedrohungen bietet.
- Falls der Partner einen eigenen Server oder eine Cloud-Umgebung nutzt, muss diese durch **Firewall-Regeln und Netzwerksicherheitsmechanismen** abgesichert sein.
- Alle externen Zugriffsmöglichkeiten auf Server (z. B. SSH, RDP) müssen gesichert sein.

1.3. Domain & Zertifikate

- Die Partner-Website muss unter einer eigenen **vollqualifizierten Domain (FQDN)** betrieben werden.
- **TLS-Verschlüsselung (mindestens TLS 1.2 oder höher) ist verpflichtend**, und es dürfen keine unsicheren HTTP-Verbindungen genutzt werden.
- SSL/TLS-Zertifikate müssen von einer vertrauenswürdigen Zertifizierungsstelle (CA) stammen und regelmäßig erneuert werden.

1.4. Firewall & Schutzmaßnahmen

- Die Partner müssen eine **Web Application Firewall (WAF)** oder eine vergleichbare Schutzmaßnahme einsetzen, um Angriffe wie SQL-Injection, XSS oder CSRF zu verhindern.
- Falls ein Reverse Proxy genutzt wird, muss sichergestellt sein, dass keine sicherheitskritischen Header (z. B. Authorization, X-Frame-Options, Referrer-Policy) verändert oder entfernt werden.

1.5. Einbindung

- Der Partner darf die bereitgestellten JavaScript-Widgets nicht modifizieren oder manipulieren, es sei denn, dies ist ausdrücklich erlaubt.
- Die Integration der Widgets muss entsprechend der bereitgestellten Dokumentation erfolgen.
- Der Partner darf keine zusätzlichen Caching-Mechanismen einsetzen, die zu einer veralteten Version der Widgets führen könnten.

2. Sicherheitsanforderungen

2.1. Sichere Einbindung der Widgets

- Widgets dürfen nur auf autorisierten Domains eingebunden werden, die vorab mitgeteilt und genehmigt wurden.

2.2. Schutz vor Code-Manipulation

- Widgets dürfen **nicht durch externe Skripte oder Browser-Plugins manipuliert oder verändert** werden.
- Die Partner-Website darf keine Skripte enthalten, die **aktive Code-Injection** auf Widgets oder die API-Schnittstellen vornehmen.
- Es dürfen keine **Eval()- oder dynamischen Code-Execution-Mechanismen** verwendet werden, die die Widgets unkontrolliert ausführen könnten.

2.3. Monitoring & Incident Response

- Sicherheitsvorfälle, die das Widget oder die API betreffen, müssen **unverzüglich** gemeldet werden, einschließlich:
    - Kompromittierung der Infrastruktur
    - API-Schlüssel-Leaks
    - Unerlaubte oder verdächtige Manipulationen an unserer Codebasis

2.4. Authentifizierungsverfahren

- Der Partner muss für Stufe-2-Widgets ein O-Auth-Authentifizierungsverfahren bereitstellen. Sollte der Partner ein solches Verfahren nicht zur Verfügung stellen könne, kann die Gründerplattform bei der Einrichtung unterstützen. Bitte kontaktieren Sie uns in diesem Fall.

Stand März 2025