

Wellness Muster AG

Was Ihr Assistent im September 2026 geleistet hat – und wie er überwacht wurde.

142

Anrufe beantwortet

38

Termine am Telefon gebucht

58

Online-Buchungen

6

Vorfälle abgewehrt

Telefonassistent

Anrufe beantwortet	142
Gesprächsminuten insgesamt	331
Durchschnittliche Gesprächsdauer	2.3 Minuten
An eine Person weitergeleitet	6
Termine gebucht / verschoben / storniert	38 / 4 / 5
Verfügbarkeiten abgefragt	61

Online-Buchung

Buchungen insgesamt	103
davon online / am Telefon / vom Betrieb eingetragen	58 / 38 / 7
Stornos durch Gäste / durch den Betrieb	6 / 2
Nachrichten nicht zugestellt	0
Vom Missbrauchsschutz gebremst	3

Sicherheit

Ihr Assistent wird laufend überwacht – ausgerichtet an den «OWASP Top 10 for Agentic Applications», der Liste der wichtigsten Sicherheitsrisiken für KI-Assistenten der gemeinnützigen OWASP-Stiftung. Acht der zehn Kategorien betreffen einen Telefonassistenten, zwei nicht; beide stehen der Vollständigkeit halber mit Begründung da.

ASI01	Agent Goal Hijack	Anweisungsartige Äußerungen von Anrufern im Gesprächsverlauf	1 Anweisungsversuch von Anrufern erkannt und gemeldet.
ASI02	Tool Misuse	Änderungen von fremder Nummer, mehrere Änderungen in einem Anruf	2 Änderungen von einer fremden Nummer abgewehrt – der Termin blieb unverändert.
ASI03	Identity & Privilege Abuse	Abgewiesene Zugriffe, Aufrufe ohne zuordenbaren Betrieb	Keine Auffälligkeiten.
ASI04	Supply Chain	Abweichung des Assistenten von der provisionierten Konfiguration	An 30 Tagen geprüft, jedes Mal wie vorgesehen.

ASI05	Unexpected Code Execution	–	Nicht anwendbar: Der Telefonassistent führt keinen Code aus.
ASI06	Memory & Context Poisoning	Anweisungsartiger Text in Buchungsfeldern (Web wird Telefon-Kontext)	Keine Auffälligkeiten.
ASI07	Insecure Inter-Agent Communication	–	Nicht anwendbar: Ein einzelner Agent – keine Kommunikation zwischen Agents.
ASI08	Cascading Failures	Fehlerquote der Werkzeuge, gescheiterte Mails, SMS und Rückerstattungen	Keine Ausfälle.
ASI09	Human-Agent Trust Exploitation	Verhinderte Preisgabe fremder Daten, Notfall ohne Weiterleitung	Keine fremden Daten preisgegeben; 1 Anfrage ohne passende Nummer verweigert.
ASI10	Rogue Agents / Drift	Abweichung von der Grundlinie: Anrufzahl und Gesprächsdauer	Verhalten im üblichen Rahmen.

Warnungen in diesem Monat

11.09. · Ein Anrufer hat versucht, dem Assistenten Anweisungen zu geben – erledigt

Was dafür gespeichert wird

Nur, was geschah, wann und mit welchem Ergebnis – keine Gesprächsinhalte, keine Namen, keine Telefonnummern. Anrufernummern werden höchstens als unumkehrbare Prüfsumme verglichen. Aufbewahrung 90 Tage, Server in Deutschland.

Silvio Peng · unavox · 8602 Wangen ZH · unavox.ch · info@unavox.ch