IT TALK

General Solutions
SOFTWARE

Handout: Fragenkatalog Cybersecurity

Verantwortung nach NIS2: Die Verantwortung für Cybersicherheit liegt bei der Geschäftsleitung, nicht beim IT-Dienstleister. Die Geschäftsleitung genehmigt die Sicherheitsmaßnahmen, überwacht ihre Umsetzung und haftet bei Versäumnissen (NIS2-Richtlinie, Art. 20). Der IT-Dienstleister setzt um, die Verantwortung lässt sich nicht delegieren. Gehen Sie diesen Katalog gemeinsam mit Ihrem IT-Dienstleister Punkt für Punkt durch. Die Antworten prüft und verantwortet das Unternehmen selbst.

Bitte lassen Sie jede Frage schriftlich beantworten. Eine Antwort wie „Das haben wir im Griff“ gilt nicht. Fehlt ein Nachweis, gilt der Punkt als offen.

Hinweis: Diese Liste ist ein Anhaltspunkt und nicht vollständig. Sie ersetzt weder eine individuelle Sicherheitsprüfung noch eine Beratung.

NR.	BEREICH	FRAGE AN DEN IT-DIENSTLEISTER	BEISPIELANTWORT	STATUS
1	**Notfallplan und Erreichbarkeit**	Gibt es einen schriftlichen Notfallplan auf Papier, mit Zuständigkeiten, Telefonnummern und Entscheidungsbefugnis? Wer ist am Samstag um 6 Uhr erreichbar, und in welcher Zeit sind Sie bei uns?	Aktueller Plan, im letzten Jahr geübt. Reaktionszeit vertraglich festgelegt.	☐ ok ☐ offen
2	**Firewall und Netzwerk**	Welche Firewall ist im Einsatz, wer pflegt sie, und wann wurden Regeln und Firmware zuletzt geprüft? Sind Gäste-WLAN, Kassensystem, Schlüsselkarten und Büro-Netz voneinander getrennt?	Gepflegte Firewall mit aktueller Firmware, dokumentierte Netzwerktrennung, keine offenen Ports ohne Begründung.	☐ ok ☐ offen
3	**Physische Sicherheit**	Wer hat physischen Zugang zu Server, Firewall und Netzwerkschränken? Ist der Raum verschlossen und für externe Dienstleister, etwa Handwerker, tabu?	Eigener, abgesperrter Raum, Zutrittsliste, Schlüsselverwaltung, kein Zugang ohne Begleitung.	☐ ok ☐ offen
4	**Fernzugänge und VPN**	Wo gibt es Fernzugänge (VPN, Fernwartung, Portfreigaben)? Welche davon sind mit Zwei-Faktor-Anmeldung geschützt? Wer von Ihren Dienstleistern hat Zugriff?	Jeder Zugang mit Zwei-Faktor-Anmeldung, personalisierte Konten, Zugänge von Dienstleistern befristet und protokolliert.	☐ ok ☐ offen

NR.	BEREICH	FRAGE AN DEN IT-DIENSTLEISTER	BEISPIELANTWORT	STATUS
5	**Endpoint Security**	Welche Endpoint Security läuft auf Arbeitsplätzen und Servern, und gehören EDR (Endpoint Detection & Response) und XDR (Extended Detection & Response) dazu? Wer wertet Alarme aus, auch nachts und am Wochenende? Ist der Manipulationsschutz aktiv?	Endpoint Security mit EDR/XDR auf allen Geräten inklusive Server, Alarmauswertung rund um die Uhr (MDR), unabhängige Testergebnisse des Produkts vorlegbar.	☐ ok ☐ offen
6	**Updates und Patches**	Wie schnell werden kritische Sicherheitsupdates eingespielt: Betriebssystem, Server, Firewall, Buchungs- und Kassensoftware? Gibt es eine Liste aller Systeme?	Kritische Updates binnen Tagen, vollständige Systemübersicht, veraltete Systeme isoliert.	☐ ok ☐ offen
7	**Mobile Geräte**	Wie werden Tablets, Smartphones und mobile Kassen verwaltet? Lassen sie sich bei Verlust aus der Ferne löschen (Remote Wipe), und sind die Daten darauf verschlüsselt?	Zentrale Geräteverwaltung (MDM), Remote Wipe getestet, Verschlüsselung und Gerätesperre Pflicht.	☐ ok ☐ offen
8	**Konten und Berechtigungen**	Ist Zwei-Faktor-Anmeldung für E-Mail, Buchungsplattformen und Administratoren aktiv? Sind Administratorkonten von normalen Konten getrennt? Gibt es geteilte Zugänge?	Zwei-Faktor-Anmeldung überall, getrennte Admin-Konten, keine geteilten Zugänge, Passwort-Manager im Einsatz.	☐ ok ☐ offen
9	**Cloud und Microsoft 365**	Wer prüft die Konfiguration von Microsoft 365 oder Google Workspace, etwa Conditional-Access-Richtlinien und das Blockieren veralteter Anmeldeprotokolle? Business Email Compromise läuft heute meist über die Cloud. Wie oft wird die Konfiguration kontrolliert (Secure Score, Audit)?	Regelmäßige, dokumentierte Konfigurationsprüfung, Conditional Access aktiv, veraltete Protokolle gesperrt, Ergebnisse schriftlich vorhanden.	☐ ok ☐ offen
10	**Cloud: Anmeldung und Administratoren**	Wer hat Administratorrechte in der Cloud? Ist Zwei-Faktor-Anmeldung für alle Konten erzwungen, auch für Administratoren und Dienstleister? Werden Anmeldungen aus dem Ausland, unmögliche Ortswechsel und neue Weiterleitungsregeln im Postfach überwacht?	Wenige, namentliche Admin-Konten mit starker Anmeldung, Warnungen bei verdächtigen Anmeldungen und Postfachregeln, Zugriff von Dienstleistern befristet.	☐ ok ☐ offen
11	**Cloud: Daten und Backup**	Welche Daten liegen in der Cloud (E-Mail, Dateien, Buchungs- und Kassensystem)? Wer sichert sie? Cloud-Anbieter sichern ihre Plattform, nicht automatisch unsere Daten. Wie lange und wie vollständig lassen sich gelöschte Daten wiederherstellen?	Eigenes, vom Anbieter getrenntes Backup der Cloud-Daten, Wiederherstellung getestet, Speicherort und Aufbewahrung bekannt.	☐ ok ☐ offen
12	**Cloud: Dienste und Freigaben**	Welche Cloud-Dienste setzen wir ein (Buchungsplattformen, Channel Manager, Gäste-Apps)? Wer ist dafür verantwortlich? Gibt es öffentliche Freigabelinks auf Dateien mit Gäste- oder Mitarbeiterdaten?	Vollständige Liste aller Dienste mit Verantwortlichen, Freigaben regelmäßig bereinigt, Sicherheitsnachweise der Anbieter liegen vor.	☐ ok ☐ offen
13	**Cloud: Datensouveränität**	In welchem Land und Rechtsraum liegen unsere Daten? Gibt es Auftragsverarbeitungsverträge nach DSGVO? Wer außerhalb der EU, etwa Anbieter mit Sitz in den USA, kann auf Daten zugreifen? Wer hält die Schlüssel zur Verschlüsselung?	Speicherort Europa vertraglich festgelegt, Auftragsverarbeitungsverträge vorhanden, Zugriffsrechte des Anbieters bekannt, bei sensiblen Daten eigene Schlüssel.	☐ ok ☐ offen

NR.	BEREICH	FRAGE AN DEN IT-DIENSTLEISTER	BEISPIELANTWORT	STATUS
14	**Cloud: Abhängigkeit (Lock-in)**	Was geschieht, wenn der Anbieter ausfällt, die Preise erhöht oder wir wechseln wollen? Lassen sich alle Daten vollständig und in offenen Formaten exportieren? Gibt es eine Ausstiegsstrategie und eine Notlösung für einen längeren Ausfall?	Regelmäßiger Datenexport in offenen Formaten, dokumentierte Ausstiegsstrategie, Kündigungs- und Rückgabebedingungen vertraglich geregelt, Notbetrieb ohne Cloud geübt.	☐ ok ☐ offen
15	**Offboarding von Mitarbeitern**	Wie schnell und in welchem Prozess werden Zugänge (E-Mail, Buchungssystem, Kassensystem) gesperrt, wenn Mitarbeiter ausscheiden? Bleiben alte Konten als Zombies offen?	Festgelegter Prozess, Sperrung am letzten Arbeitstag, regelmäßige Bereinigung inaktiver Konten.	☐ ok ☐ offen
16	**E-Mail-Schutz**	Welcher Phishing- und Spam-Schutz ist aktiv, werden Anhänge geprüft, und sind SPF, DKIM und DMARC für unsere Domain eingerichtet?	Filter aktiv und geprüft, DMARC nicht nur im Beobachtungsmodus.	☐ ok ☐ offen
17	**User Awareness**	Wann wurden Rezeption und Team zuletzt geschult? Gibt es Phishing-Simulationen? Gibt es eine Regel und einen Meldeweg für verdächtige Mails von Gästen und Buchungsplattformen?	Schulung mindestens jährlich, Rezeption gesondert, Meldeweg ohne Schuldzuweisung.	☐ ok ☐ offen
18	**Schatten-IT**	Wird verhindert oder überwacht, dass Mitarbeiter nicht genehmigte Cloud-Dienste (private Dropbox, WhatsApp) für betriebliche Zwecke nutzen, etwa für Gästelisten und Ausweiskopien?	Freigegebene Dienste für den Betrieb, klare Regel, technische Kontrolle.	☐ ok ☐ offen
19	**Backup und Wiederherstellung**	Gibt es eine Kopie, die vom Netz getrennt oder unveränderbar ist? Wann wurde die Wiederherstellung zuletzt getestet, und wie lange dauert ein kompletter Neuaufbau?	Offline- oder unveränderbare Kopie, dokumentierter Wiederherstellungstest, bekannte Wiederanlaufzeit.	☐ ok ☐ offen
20	**Monitoring und Protokolle**	Wer erkennt ungewöhnliche Aktivitäten im Netz? Werden Protokolle zentral gespeichert, und wie lange?	Benannte Stelle für Alarme, Protokolle über mehrere Monate verfügbar.	☐ ok ☐ offen
21	**Spurensicherung im Ernstfall**	Was passiert im Ernstfall zuerst: Server neu aufsetzen oder Ursache und Datenabfluss klären? Welcher forensische Partner steht bereit?	Erst isolieren und sichern, dann neu aufbauen. Forensik-Partner benannt.	☐ ok ☐ offen
22	**Partner und Lieferkette**	Welche Dienstleister und Softwareanbieter haben Zugriff auf unsere Daten? Welche Sicherheitsnachweise liegen vor, und welche Meldefrist gilt, wenn bei ihnen etwas passiert?	Liste aller Partner, Nachweise (zum Beispiel ISO 27001), Meldefrist im Vertrag.	☐ ok ☐ offen
23	**Meldepflichten**	Wer meldet binnen 72 Stunden an die Datenschutzbehörde, wer informiert Gäste, Kunden und andere Betroffene?	Verantwortliche Person benannt, Vorlagen vorhanden.	☐ ok ☐ offen

NR.	BEREICH	FRAGE AN DEN IT-DIENSTLEISTER	BEISPIELANTWORT	STATUS
24	**Cyberversicherung**	Gibt es eine Cyberversicherung, welche Voraussetzungen und Meldefristen verlangt sie, und steht ihre Notfallnummer im Notfallplan?	Police gelesen, Auflagen erfüllt, Notfallnummer im Plan.	☐ ok ☐ offen
25	**Daten und Verschlüsselung**	Welche Gäste- und Zahlungsdaten speichern wir, wo und wie lange? Sind sie verschlüsselt?	Nur nötige Daten, Löschkonzept, Verschlüsselung auf Geräten und Datenträgern.	☐ ok ☐ offen
26	**Unabhängige Prüfung**	Wann wurde zuletzt ein Sicherheitscheck oder Penetrationstest durch eine unabhängige Stelle durchgeführt?	Schriftliches Ergebnis, Maßnahmen mit Terminen.	☐ ok ☐ offen

Dieser Fragenkatalog wurde von **Peter Stelzhammer** erstellt. General Solutions hat ihn als Veranstalter des IT Talk 2026 lediglich in das Design der Veranstaltung übertragen.