KOM SG

Zusammenfassung – Checkliste Sicherheitsvorschriften

Auch 2019 wurde bei vielen Gemeinden das Ausfüllen der Checkliste betreffend Sicherheitsvorschriften verlangt. Ausgenommen von der Umfrage waren Gemeinden, die im Jahr 2018 oder 2019 auditiert wurden, diese müssen die Checkliste in den 2 Folgejahren nicht ausfüllen.

Erstmals wurde auf ein neues Umfragetool gesetzt, was eine Umstellung bedeutete. Es gingen dazu auch einige Verbesserungsvorschläge ein. Eine der häufigsten Anfragen betraf die Möglichkeit des Exports der Antworten. Eine entsprechende Funktion wurde in der Zwischenzeit implementiert.

Die Auswertung der Checklisten ergab im Grossen und Ganzen nicht sehr viele Änderungen zu den Vorjahren. Auffällig ist der kontinuierliche Rückgang an eigenen Exchange Mailservern. Lösungen wie Office 365 oder die Dienstleistung der Abraxas erlauben es Gemeinden den eigenen Internetzugang abzubauen. Dieser wird oftmals lediglich für die Mailserverkommunikation (ActiveSync, OWA) verwendet. Das Wegfallen des eigenen Internetzugangs reduziert die Komplexität und erhöht die Sicherheit.

Zu den Punkten mit den meisten Angaben zur nicht-Einhaltung der Vorschriften gehören unter anderem die Möglichkeit zur automatischen Weiterleitung von Emails, Testschaltungen auf Firewall-Komponenten sowie eine fehlende SSL-Inspection.

Die durchgeführten Audits zeigen teilweise eine grosse Diskrepanz zu den Angaben der Gemeinden in der Checkliste. So gaben beispielsweise fast 100% der befragten Gemeinden an, Sicherheitsupdates für Software innerhalb der geforderten Zeitspanne zu installieren, die durchgeführten Audits zeigten jedoch ein nahezu umgekehrtes Bild. Oftmals fehlt es an Wartungsverträgen mit IT-Dienstleistern, die eine fristgerechte Installation solcher Updates sicherstellen resp. spezifisch definieren (SLA).

Weiterhin zeigen durchgeführte Audits oftmals Schwachstellen in der Netzwerkumgebung, sowie bei den organisatorischen Vorgaben aus den Sicherheitsvorschriften. Wir treffen zum Beispiel häufig auf «flache» Netzwerkumgebungen sowie unvollständige Benutzerweisungen.

Nachfolgend finden Sie einige Tipps und nützliche Links zur Verbesserung der Informationssicherheit:

- Besprechen Sie das Thema Softwareaktualisierung mit Ihrem IT-Partner, vergleichen Sie aktuelles Vorgehen mit den Vorschriften und handeln Sie, wenn nötig, ein entsprechendes SLA mit dem Partner aus.
- Füllen Sie den Fragebogen in Kooperation mit Ihrem IT-Partner aus, viele technische Fragen können ansonsten nicht korrekt beantwortet werden. Nach dem Ausfüllen können Sie in Zukunft die Antworten für nächstes Jahr exportieren.
- Konsultieren Sie mit Ihrem IT-Partner folgendes Factsheet zur Netzwerksegmentierung und besprechen Sie, was davon bereits umgesetzt ist oder wie eine Segmentierung allenfalls erreicht werden könnte: https://komsg.ch/wp-content/uploads/2020/01/Netzwerksegmentierung_v1.0.pdf
- Unter folgendem Link finden Sie die aktuellen Sicherheitsvorschriften der KOM SG: https://komsg.ch/wp-content/uploads/2015/02/Sicherheitsvorschriften-KOM-SG-6.0-g%C3%BCltig-ab-20190701.pdf
- Unter folgendem Link finden Sie eine Vorlage für die Weisungen an Benutzer, diese enthält alle nötigen Inhalte um den Vorschriften gerecht zu werden: https://komsg.ch/wp-content/uploads/2015/02/Muster-Informatikweisung-V1.0.pdf