Einhaltung der vertraglichen Verpflichtungen zum IT-Grundschutz

Sehr geehrte Damen und Herren

Ihr Unternehmen erbringt IT-Dienstleistungen für unsere Gemeinde XY oder eine unserer Unterabteilungen.

Der Hackerangriff auf die Firma Xplain hat deutlich gemacht, dass der Aufrechterhaltung des Grundschutzes im Bereich Informatiksicherheit[[1]](#footnote-1) eine grössere Bedeutung beigemessen werden muss. Dasselbe gilt für die verschiedenen Sicherheitsvorfälle, die sich in den letzten Jahren in Schweizer Gemeinden ereignet haben. Der IKT-Grundschutz legt die minimalen organisatorischen, personellen und technischen Sicherheitsvorgaben verbindlich fest, wobei die Vorschriften zur Sicherheit von Personendaten (21 nGIDA[[2]](#footnote-2)) ) und zur Einhaltung der Regeln über die Vergabe von Unteraufträgen (Artikel 28b ff nGIDA ) in jedem Fall eingehalten werden müssen, was auch in den Verträgen, die wir mit Ihnen abgeschlossen haben, vorgesehen sein sollte. Eventuelle zusätzliche vertragliche Bestimmungen zur Aufrechterhaltung der Informationssicherheit, die über den grundlegenden IT-Schutz hinausgehen, müssen selbstverständlich ebenfalls beachtet werden.

Wir gehen davon aus, dass Ihr Unternehmen diesen Verpflichtungen nachkommt. Als proaktive und präventive Massnahme hat unsere Gemeinde beschlossen, von ihren wichtigsten externen Dienstleistern eine schriftliche Bestätigung zu verlangen, dass sie den grundlegenden IT-Schutz umsetzen und zu erklären, wie sie dies tun. Wir erwarten, dass bei erhöhtem Schutzbedarf, d. h. je nach Bedeutung der Daten und Dokumente und im Hinblick auf das Inkrafttreten des neuen Gesetzes über die Information der Öffentlichkeit, den Datenschutz und die Archivierung am 1. Januar 2024 (im Folgenden: "nGIDA") zusätzliche Schutzmassnahmen ergriffen werden. Dies gilt insbesondere für die Verwaltung von Produktionsdaten, die Ihnen im Rahmen der Erfüllung Ihrer Aufgaben übermittelt werden. Zu den für uns relevanten Anwendungsfällen gehören unter anderem (diese Liste ist nicht vollständig, sondern gibt einen Überblick über die relevanten Problematiken):

* Werden Produktionsdaten regelmässig gelöscht, nachdem ein Service- oder Supportfall abgeschlossen ist?
* Werden die Produktionsdatenbanken, falls sie für die Projektarbeit zwingend erforderlich sind, gemäss den nGIDA-Bestimmungen aufbewahrt? Unterliegen sie einem besonderen Schutz und werden sie nach Abschluss der Arbeiten gemäss denselben Bestimmungen endgültig gelöscht?
* Ist sichergestellt, dass die Testdatenbanken unter keinen Umständen Produktionsdaten enthalten? Die Testdatenbanken müssen systematisch anonymisiert werden. Falls dennoch Produktionsdaten in diesen Datenbanken enthalten sein sollten, werden diese Daten entsprechend geschützt, insbesondere durch Verschlüsselung, Zugriffskontrolle und Protokollierung der Zugriffe?
* Ist sichergestellt, dass für Integrationsumgebungen keine Produktionsdaten erforderlich sind? Falls dennoch Produktionsdaten benötigt werden, sind für diese Fälle zusätzliche Vorkehrungen getroffen?
* Sind Testdaten, Testdatenbanken und Testumgebungen sowie Screenshots, die Testdaten enthalten oder anonymisiert sind, klar als solche gekennzeichnet, damit sie von Produktionsdaten unterschieden werden können?
* Werden Screenshots aus den Produktionssystemen bei Projektarbeiten und Supportfällen rigoros anonymisiert? Werden die Originale systematisch gelöscht? Werden die Absender regelmässig darauf hingewiesen, dass sie nur anonymisierte Screenshots versenden dürfen?
* Sind die Protokolldateien so gestaltet, dass sie keine Kundenproduktionsdaten enthalten? Bieten sie die Möglichkeit, Kundenproduktionsdaten auf einfache Weise zu filtern oder zu anonymisieren, sodass sie im Supportfall ohne besondere Massnahmen weitergegeben werden können? Werden die Protokolldateien nach der Analyse gelöscht?
* Sind die Produktionsdaten (oder Auszüge daraus) so geschützt, dass sie nur den Mitarbeiterinnen und Mitarbeitern zugänglich sind, die sie zur Ausführung ihrer Aufgaben unbedingt benötigen? Werden sie nach Erledigung der Aufgabe gelöscht? Wird dieses Verfahren regelmässig kontrolliert?
* Sind die Dokumente unserer Gemeinde vor unberechtigtem Zugriff und Datenlecks geschützt und entsprechend ihrer Sensibilität sicher gespeichert? Wird dieses Verfahren regelmässig überprüft? Werden Dokumente, die nicht mehr benötigt werden, regelmässig gelöscht?
* Ist sichergestellt, dass bei der Softwareentwicklung keine Anmeldedaten oder Passwörter im Quellcode im Klartext lesbar sind?
* Ist sichergestellt, dass Informationen zum Systemzugriff (Benutzerkennungen, Passwörter, IP-Adressen, Ports usw.) unter keinen Umständen im Klartext in Konfigurationsdateien oder anderen Dateien gespeichert werden?
* Wie wird sichergestellt, dass Zertifikate, die zu Testzwecken verwendet werden, später nicht in der Produktion eingesetzt und nach Abschluss der Testphase gelöscht werden?
* Gibt es einen sicheren Kanal, über den sensible Daten ausgetauscht werden können, wenn dies unbedingt erforderlich ist (z. B.: über eine verschlüsselte E-Mail oder ein sicheres Portal)?
* Werden die Zugangsinformationen zu den Systemen unserer Gemeinde (Konten, Passwörter, Authentifizierungsdaten, IP-Adressen usw.) in verschlüsselter Form gespeichert?
* Wird der Zugriff von IT-Supportteams auf Produktivsysteme durch eine starke Zwei-Faktor-Authentifizierung geschützt, systematisch protokolliert und die Kommunikation verschlüsselt?
* Werden Schlüssel mit mindestens 256 Bit verwendet, um die Informationen unserer Gemeinde zu verschlüsseln?
* Sind Ihre Mitarbeiterinnen und Mitarbeiter für Cyberrisiken und die Sensibilität der Daten unserer Gemeinde sensibilisiert und geschult?

Wir bitten Sie, uns bis zum [Frist von 30 Tagen ab Versand des Schreibens] 2023 per Einschreiben Ihre detaillierten Erläuterungen (inkl. Prozessbeschreibung, Liste der Kundenproduktionsdaten (auch Artefakte wie Logfiles oder nicht anonymisierte Screenshots aus den Produktionssystemen) usw.) unter Berücksichtigung der obigen Fragen zukommen zu lassen (Postadresse: Gemeinde [XXX], Adresse, Postleitzahl, Gemeinde).

Bei Fragen können Sie sich an [Frau oder Herr] wenden:

- [Tel.-Nr.]

- [E-Mail-Adresse].

Mit freundlichen Grüssen

1. <https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren/grundschutz.html> [↑](#footnote-ref-1)
2. <https://lex.vs.ch/app/de/texts_of_law/170.2/versions/3229> . [↑](#footnote-ref-2)