Kreuzlingen

Stadtrat

Sperrfrist für alle Medien
Veröffentlichung erst nach der Medienkonferenz zur Gemeinderatssitzung

Beantwortung

Schriftliche Anfrage zu Microsofts gestohlener Master-Key und sind die kompletten Office365 und Kommunikationsdaten der Stadt Kreuzlingen und ihrer Einwohner im Internet verfügbar?

Am 16. August 2023 reichte Gemeinderat Georg Schulthess die schriftliche Anfrage zu "Microsofts gestohlener Master-Key und sind die kompletten Office365 und Kommunikationsdaten der Stadt Kreuzlingen und ihrer Einwohner im Internet verfügbar?" ein (Beilage).

Der Stadtrat beantwortet die Fragen wie folgt:

1 In welcher Form und in welchem Ausmass ist die Stadt Kreuzlingen davon betroffen?
Gemäss einer Analyse (Investigation of Storm-0558 specific indicators of compromise [IOC]) der InfoGuard AG gab es keine unberechtigten Zugriffe, die auf das Master-Key-Problem zurückzuführen sind. Die Stadtverwaltung arbeitet seit 2022 in Sachen IT-Sicherheit mit der InfoGuard AG zusammen. Die InfoGuard AG ist spezialisiert auf umfassende Cyber Security. Ihre 360°-Expertise reicht von Cyber Defence Services und Incident Response Services über Managed Security & Network Solutions für IT-, OT- und Cloud-Infrastrukturen bis hin zu Services in den Bereichen, Engineering, Penetration Testing & Red Teaming sowie Security Consulting. Die Cloud-, Managed- und SOC-Services erbringt der Schweizer Cyber-Security-Experte aus dem ISO 27001-zertifizierten und ISAE 3000 Typ 2 überprüften Cyber Defence Center in der Schweiz. InfoGuard AG, mit Hauptsitz in Baar/Zug sowie Niederlassungen in Bern, München und Wien, schützt rund um die Uhr mehr als 400 Kundinnen und Kunden in der Schweiz, Deutschland und Österreich. Dafür sorgen über 230 Sicherheitsfachleute. Zu den Kundinnen und Kunden zählen namhafte Banken, Versicherungen, Industrieunternehmen, Energiedienstleister, Spitäler, Handelsunternehmen, Service Provider und Behörden. Das Unternehmen ist ISO/IEC 27001:2022 sowie ISO 14001 zertifiziert, Mitglied bei FIRST (Global Forum of Incident Response and Security Teams) und BSI-qualifizierter APT-Response-Dienstleister.

2 Wurden seitens der Informatik der Stadt Kreuzlingen die auf Drängen der Microsoft-Kunden nun doch noch bereitgestellten Logdateien auf unberechtigte Zugriffe geprüft?
Ja, durch externe Fachpersonen der InfoGuard AG wurden die Logs analysiert. Es wurden keine unberechtigten Zugriffe gefunden.

3 Sind Daten der Stadt Kreuzlingen im Darknet aufgetaucht / zum Kauf angeboten worden?
Da von externen Fachpersonen keine Hinweise auf unberechtigte Zugriffe gefunden wurden, wurde auf eine Darknet-Analyse verzichtet.

4 Hat die Stadt Kreuzlingen mit Microsoft zur Klärung Kontakt aufgenommen?
Gemäss Microsoft wurden alle betroffenen Kundinnen und Kunden kontaktiert. Die Stadt Kreuzlingen hat jedoch keine entsprechende Mitteilung erhalten.

5 Wenn betroffen, hat sich die Stadt Kreuzlingen als Kunde der Firma Microsoft über die stark ungenügende Qualität und Sicherheit der Dienstleistung beschwert, Verbesserung gefordert? (Diese Dienstleistung kostet die Stadt Kreuzlingen wiederkehrend 84'122.95 CHF pro Jahr)
Da die Stadt Kreuzlingen vom Problem nicht betroffen ist, hat sie sich diesbezüglich nicht beschwert.

Die Kosten in Höhe von CHF 84'000.– setzen sich vorwiegend aus Arbeitsplatz- und einigen Cloud-Lizenzen zusammen.

6 Gedenkt die Stadt Kreuzlingen ihre Einwohner über diesen Vorfall zu informieren? (Ob betroffen oder nicht)
Die Stadt Kreuzlingen steht ein für eine aktive und offene Kommunikation. Da die Stadtverwaltung bzw. die Informatik der Stadt nicht von unberechtigten Zugriffen betroffen ist oder war, besteht oder bestand aus der Sicht des Stadtrats keine Notwendigkeit für eine Kommunikation.

7 Wer ist in der Gemeinde Kreuzlingen Datenschutzbeauftragter und ist diese Stelle durch eine vom Betrieb der Stadt unabhängige Person besetzt? Hat der Datenschutzbeauftragte in diesem Falle etwas unternommen?
Die erste Anlaufstelle der Gemeinde ist der Stadtschreiber. Diese Person klärt gegebenenfalls unter Einbezug juristischer Unterstützung den Sachverhalt. Dabei kann der Datenschutzbeauftragte des Kantons Thurgau konsultiert werden. Oder es wird externe juristische Unterstützung beigezogen. Aktuell arbeitet die Stadtkanzlei mit Rechtsanwalt Christophe Steiger von der Kanzlei Raggenbass zusammen.

Da wie in den obigen Fragestellungen geschildert keine Datenschutzverletzung an die Stadt herangetragen wurde, wurden auch seitens Stadt keine Schritte unternommen.

8 Welche Massnahmen will die Stadt Kreuzlingen in Zukunft treffen, um die Daten der Kreuzlinger Einwohner und der Verwaltung zu schützen?
Während der Corona-Pandemie wurden aus der Notwendigkeit heraus Microsoft-365-Dienste, darunter Teams, implementiert. Die Stadt evaluiert kontinuierlich Massnahmen, um die Daten der Einwohnerinnen und Einwohner von Kreuzligen zu schützen. Derzeit wird in Zusammenarbeit mit externen Fachpersonen eine umfassende Richtlinie für die Nutzung der Microsoft-365-Dienste erarbeitet.

9 Auf welche Gesetzesgrundlage stützt die Stadt Kreuzlingen die Nutzung solcher Clouds obwohl diese gemäss Datenschutzgesetz für die öffentliche Hand nicht genutzt werden dürfte?
Zunächst ist klarzustellen, dass das Datenschutzgesetz die Nutzung von Clouds durch die öffentliche Hand nicht verbietet.

In Bezug auf den Datenschutz untersteht die Stadt Kreuzlingen als "öffentliches Organ" dem kantonalen Gesetz über den Datenschutz vom 9. November 1987 (TG DSG).[1] Die Auslagerung von Daten in einen Cloud-Dienst gilt als Auftragsdatenbearbeitung durch verwaltungsexterne Dritte (sog. "Bearbeiten im Auftrag").[2] Diese ist, gestützt auf § 12 Abs. 1 TG DSG, zulässig. Die Auslagerung von Datenbearbeitungen in einen Cloud-Dienst gilt nicht als Bekanntgabe von Personendaten an Dritte im Sinne von § 9 TG DSG und bedarf demzufolge weder einer weitergehenden gesetzlichen Ermächtigung noch der Zustimmung der betroffenen Personen.[3] Andernfalls würde § 12 TG DSG, der das Outsourcing ermöglichen soll, geradezu ausgehebelt.[4]

Der Anbieter des Cloud-Dienstes ist als Hilfsperson der Stadt Kreuzlingen gemäss Art. 320 Ziffer 1 des Schweizerischen Strafgesetzbuches (StGB) zu betrachten, weshalb auch das Amtsgeheimnis bei einer Auslagerung von Daten in einen Cloud-Dienst nichts entgegensteht.[5] Ausserdem hat die Stadt Kreuzlingen vertraglich sichergestellt, dass sich der Anbieter des Cloud-Dienstes seiner Stellung als Hilfsperson der Stadt Kreuzlingen bewusst ist (siehe dazu unten).

---

1 § 2 Abs. 2 Ziffer 1 TG DSG lautet wie folgt: *«Den Bestimmungen dieses Gesetzes unterstehen als öffentliche Organe im Sinne dieses Gesetzes: 1. der Staat, die Gemeinden, die Organisationen des kantonalen öffentlichen Rechtes mit eigener Rechtspersönlichkeit und die Personen, die mit öffentlichen Aufgaben dieser Gemeinwesen betraut sind, seien sie Behördemitglieder, Beamte oder Angestellte, seien sie vollamtlich, nebenamtlich, ständig oder vorübergehend tätig; […]»*.

2 Siehe dazu insbesondere Botschaft des Regierungsrats vom 15.12.1987 zum TG DSG, S. 8, Ziffer II; Datenschutzbeauftragte des Kantons Zürich, Leitfaden zur Nutzung externer Cloud-Dienste, https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_nutzung_externer_cloud_dienste.pdf, S. 1.

3 Siehe dazu wiederum Botschaft des Regierungsrats vom 15.12.1987 zum TG DSG, S. 8, Ziffer II, wo § 12 TG DSG nicht unter den Bestimmungen über die Bekanntgabe von Daten aufgeführt ist.

4 Siehe dazu mangels Kommentars zum TG DSG zur vergleichbaren Situation im Kanton Basel-Stadt: Beat Rudin (Datenschutzbeauftragter des Kantons Basel-Stadt), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt (IDG), Rz. 12 zu § 7.

5 Siehe dazu insbesondere Bericht der Bundeskanzlei der Schweizerischen Eidgenossenschaft, Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung, https://www.bk.admin.ch/dam/bk/de/dokumente/dti/themen/cloud/rechtsrahmen.pdf.download.pdf/Rechtlicher%20Rahmen%20f%C3%BCr%20die%20Nutzung%20von%20Public-Cloud-Diensten%20in%20der%20Bundesverwaltung%20%28inkl.%20Anh%C3%A4nge%20A%20und%20B%29.pdf, Ziffer 2.

Zwar besteht gegenwärtig eine Kontroverse mit Bezug auf den Zugriff im Rahmen der Verfolgung schwerer Straftaten (z. B. Cyberkriminalität, Diebstahl von Geschäftsgeheimnissen oder Terrorismus) durch US-Behörden auf Daten, die in einem Cloud-Dienst eines Anbieters mit Sitz oder Muttergesellschaft in den USA liegen (sog. "Lawful Access"). Diese ist jedoch für die Fallkonstellation, in der die eingangs genannte Frage gestellt wird, nicht relevant, und hat im Übrigen verschiedene kantonale Regierungen nicht davon abgehalten, sich für eine Nutzung des Cloud-Dienstes "Microsoft 365" auszusprechen. So haben sich insbesondere der Regierungsrat des Kantons Zürich[6] und der Regierungsrat des Kantons Thurgau[7] in jüngster Vergangenheit für eine Nutzung des Cloud-Dienstes "Microsoft 365" ausgesprochen, wobei der Regierungsrat des Kantons Zürich explizit auch die Nutzung durch die Kantonspolizei zugelassen hat.[8]

Im Rahmen einer sorgfältigen Risikoanalyse ist der Regierungsrat des Kantons Zürich mit Bezug auf die Datensicherheit zum Schluss gekommen, dass die Risiken für die Datensicherheit bei "Microsoft 365" zumindest nicht höher sind als beim Betrieb eines eigenen Rechenzentrums (sog. On-Premise-Lösung).[9] Berücksichtigt wurde unter anderem auch der Umstand, dass namhafte Softwarehersteller wie Microsoft den Support für lokal betriebene Anwendungen sukzessive zurückfahren oder ganz einstellen und dass der für Digitalisierungsvorhaben zentrale Dienst "Microsoft Teams" ausschliesslich als Cloud-Dienst angeboten wird.[10]

Der Entscheid, die Bearbeitung von Daten teilweise in einen Cloud-Dienst auszulagern, wurde vom Stadtrat der Stadt Kreuzlingen getroffen, gestützt auf eine konkrete Entscheidungsgrundlage, nämlich das Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) vom 24. August 2022, das nach der Hermes-Methode erstellt wurde. In diesem Konzept wurden zur Sicherstellung des Datenschutzes alle relevanten Risikofaktoren nach Eintretenswahrscheinlichkeit und Schadensausmass bewertet, Massnahmen zur Reduzierung dieser Risiken definiert und das verbleibende Restrisiko bestimmt, das mit einer Auslagerung einer Datenbearbeitung in einen Cloud-Dienst und der Organisation verbunden ist. Das ISDS-Konzept wird im Übrigen auch im Kanton Zürich praktiziert.[11]

Die Stadt Kreuzlingen hat sodann gemäss § 12 Abs. 1 und § 9a TG DSG vertraglich sichergestellt, dass der Datenschutz trotz Auslagerung von Datenbearbeitungen in einen Cloud-Dienst angemessen ist. Insbesondere hat sie aufgrund des Umstands, dass es sich bei Microsoft letztendlich um einen US-Konzern handelt, ungeachtet der Tatsache, dass die Daten in einem lokalen Rechenzentrum in der Schweiz gespeichert sind und der Vertrag mit der irischen Gesellschaft von Microsoft geschlossen wurde, auch die Vorgaben bezüglich des grenzüberschreitenden Datenverkehrs gemäss § 9a TG

---

6 Siehe Beschluss des Regierungsrates des Kantons Zürich vom 30. März 2022, Einsatz von Cloud-Lösungen in der kantonalen Verwaltung, (Microsoft 365), Zulassung (RRB 542/2022), https://www.zh.ch/de/politik-staat/gesetze-beschluesse/beschluesse-des-regierungsrates/rrb/regierungsratsbeschluss-542-2022.html.

7 Siehe Pressemitteilung des Regierungsrates des Kantons Thurgau vom 31. August 2023, Kantonale Verwaltung führt Microsoft 365 ein, https://www.tg.ch/news.html/485/news/65622.

8 Siehe Beschluss des Regierungsrates des Kantons Zürich vom 30. März 2022, am Ende.

9 Siehe Beschluss des Regierungsrates des Kantons Zürich, S. 3 sowie S. 7 f.

10 Siehe Beschluss des Regierungsrates des Kantons Zürich, S. Ziff. 1 und 2.

11 Siehe Leitfaden der Datenschutzbeauftragten des Kantons Zürich zur Nutzung externer Cloud-Dienste, Ziff. 5.

DSG beachtet, weil die USA, im Gegensatz zur Republik Irland, nicht Vertragspartei des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten sind. Sie unterstellte sich zu diesem Zweck dem Rahmenvertrag 2022-2025 zwischen der Schweizerischen Informatikkonferenz (SIK) und Microsoft. Dieser soll es insbesondere Verwaltungen in der Schweiz ermöglichen, die Microsoft-365-Dienste zu nutzen, indem mit Microsoft zusätzliche Bedingungen vereinbart wurden, die den spezifischen Anforderungen von öffentlichen Organen an Cloud-Dienste Rechnung tragen (z. B. Amtsgeheimnis, Gerichtsstand, etc.). Der Rahmenvertrag wurde im Übrigen unter Einbezug der Konferenz der schweizerischen Datenschutzbeauftragten (privatim) verhandelt, der auch der Datenschutzbeauftragte des Kantons Thurgau angehört.

Zusammenfassend ist somit festzuhalten, dass das Datenschutzgesetz die Nutzung öffentlicher Clouds durch die Stadt Kreuzlingen nicht verbietet und die Vorgaben des Datenschutzgesetzes an die Auslagerung von Datenbearbeitungen in einen Cloud-Dienst mit US-Muttergesellschaft eingehalten werden, insbesondere die Vorgaben an die Auftragsdatenbearbeitung durch verwaltungsexterne Dritte und den grenzüberschreitenden Datenverkehr. Zusätzlich ist anzumerken, dass sensible Daten (z. B. Einwohnerdaten und Steuerdaten) entweder intern auf Servern der Stadt oder in den Rechenzentren der Abraxas Informatik AG in Lupfig und Glattbrugg gespeichert werden.

10 Besteht diesbezüglich Kontakt zum Datenschutzbeauftragten des Kantons Thurgau?
Nein.

11 Anlässlich der Gemeinderatssitzung vom 7. Oktober 2021 stellte GR Schulthess unterstützt von GR Schläpfer den begründeten Antrag weg von Office365 Cloudlizenzen zurückzukehren zu den lokal installierten Officeprodukten. Stadtpräsident Niederberger vertrat in der Sitzung dagegen folgende Position:
Auszug aus dem Wort-Protokoll der 18. Gemeinderatssitzung vom 7. Oktober 2021:
STP Niederberger: "...Es ist auch so, dass die Services und die Sicherheitsdienste ebenfalls gewährleistet werden, was schlussendlich auch unsere interne IT entlastet. Wir haben Vorteile beim ganzen Package, dass wir ein Rundumpaket haben, wo wir alle Angebote, die Microsoft hat, nutzen können und immer vermehrt nutzen und auch intensiv nutzen. Wir haben auf der einen Seite die Cloud, die in der Schweiz gespeichert ist, wir haben Sicherheitsvorkehrungen, die gewährleistet sind und das alles mit der SIK abgesichert über Verträge.»
Der Antrag von GR Schulthess wurde mit 2 Ja-Stimmen gegen 20 Nein-Stimmen bei 17 Enthaltungen abgelehnt.
Da es sich nicht um eine konkrete Frage handelt, wird auf eine Antwort verzichtet und auf die folgende Frage 12 verwiesen.

12 Kommt Stadtpräsident Niederberger auf seine Aussage "dass die Sicherheit gewährleistet ist" zurück?
Um mit den fortschreitenden Entwicklungen Schritt zu halten, setzen viele Organisationen, darunter auch Behörden wie der Kanton Thurgau, vermehrt auf Clouddienste von Microsoft. Die Microsoft-Cloud, die von Tausenden von Sicherheitsexperten weltweit betreut wird, gewährleistet die Sicherheit der gespeicherten Daten. Im Gegensatz dazu verfügt die Stadtverwaltung Kreuzlingen nicht über eigene Sicherheitsexperten, die ausschliesslich für Sicherheitsbelange zuständig und entsprechend ausgebildet sind.

Tatsache ist, dass die Stadt Kreuzlingen in der Vergangenheit aber auch in der Zukunft alles unternehmen wird, die Sicherheit ihrer Daten zu gewährleisten. Aber wie immer wieder Beispiele in Unternehmen auf der ganzen Welt zeigen, gibt es keine absolute Sicherheit.

Kreuzlingen, 9. Januar 2024

Stadtrat Kreuzlingen

Thomas Niederberger, Stadtpräsident

Michael Stahl, Stadtschreiber

Beilage
– Schriftliche Anfrage

Mitteilung an
– Mitglieder des Gemeinderats
– Medien

Aufrecht – Kreuzlingen
Romanshornerstrasse 134
8280 Kreuzlingen
GR Georg Schulthess
georg.schulthess@aufrecht-thurgau.ch

AUFRECHT SCHWEIZ

16. August 2023

Schriftliche Anfrage zu

Microsofts gestohlener Master-Key und sind die kompletten Office365 und Kommunikationsdaten der Stadt Kreuzlingen und Ihrer Einwohner im Internet verfügbar?

Sehr geehrter Herr Präsident

Ich reiche Ihnen gestützt auf Art. 49 der derzeit gültigen Geschäftsordnung des Gemeinderates zuhanden des Stadtrates folgende schriftliche Anfrage ein:

Begründung
Im Zusammenhang mit einem der grössten Datensicherheitsdebakel der letzten Jahre, dem Diebstahl des Master-Keys der Microsoft Cloud stellen sich für die Stadt Kreuzlingen als Kunde dieser Office365 Cloud einige Fragen.

Mitte Juni wurden seltsame Vorgänge in Microsoft Online-Exchange-Konten öffentlich. Die anschliessende Analyse enthüllte ein Debakel: Mutmasslich chinesische Angreifer hatten sich Zugriff auf das von Microsoft gehostete Exchange Online vornehmlich von Regierungsbehörden verschafft. Der gestohlene Schlüssel funktionierte als Masterkey für grosse Teile der Microsoft-Cloud, in der Fachwelt wird vermutet für die komplette Cloud, also auch für Dokumente. Microsoft verweigerte sich bisher entgegen gesetzlicher Vorschriften einer transparenten Information über das Ausmass des Vorfalles.

Dazu bitten wir den Stadtrat folgende Fragen zu beantworten:

1) In welcher Form und in welchem Ausmass ist die Stadt Kreuzlingen davon betroffen?

2) Wurden Seitens der Informatik der Stadt Kreuzlingen die auf Drängen der Microsoft-Kunden nun doch noch bereitgestellten Logdateien auf unberechtigte Zugriffe geprüft?

3) Sind Daten der Stadt Kreuzlingen im Darknet aufgetaucht / zum Kauf angeboten worden?

4) Hat die Stadt Kreuzlingen mit Microsoft zur Klärung Kontakt aufgenommen?

5) Wenn betroffen, hat sich die Stadt Kreuzlingen als Kunde der Firma Microsoft über die stark ungenügende Qualität und Sicherheit der Dienstleistung beschwert, Verbesserung gefordert? (Diese Dienstleistung kostet die Stadt Kreuzlingen wiederkehrend 84'122.95 CHF pro Jahr)

6) Gedenkt die Stadt Kreuzlingen ihre Einwohner über diesen Vorfall zu informieren? (Ob betroffen oder nicht).

7) Wer ist in der Gemeinde Kreuzlingen Datenschutzbeauftragter und ist diese Stelle durch einen vom Betrieb der Stadt unabhängigen Person besetzt? Hat der Datenschutzbeauftragte in diesem Falle etwas unternommen?

8) Welche Massnahmen will die Stadt Kreuzlingen in Zukunft treffen um die Daten der Kreuzlinger Einwohner und der Verwaltung zu schützen?

9) Auf welche Gesetzesgrundlage stützt die Stadt Kreuzlingen die Nutzung solcher Clouds obwohl diese gemäss Datenschutzgesetz für die öffentliche Hand nicht genutzt werden dürfte?

10) Besteht diesbezüglich Kontakt zum Datenschutzbeauftragten des Kantons Thurgau?

11) Anlässlich der Gemeindratssitzung vom 7. Oktober 2021 stellte GR Schulthess unterstützt von GR Schläpfer den begründeten Antrag weg von Office365 Cloudlizenzen zurückzukehren zu den lokal installierten Officeprodukten. Stadtpräsident Niederberger vertrat in der Sitzung dagegen folgende Position:

Auszug aus dem Wort-Protokoll der 18. Gemeinderatssitzung vom 7. Oktober 2021:

STP Niederberger *«...Es ist auch so, dass die Services und die **Sicherheitsdienste ebenfalls gewährleistet werden**, was schlussendlich auch unsere interne IT entlastet. Wir haben Vorteile beim ganzen Package, dass wir ein Rundumpaket haben, wo wir alle Angebote, die Microsoft hat, nutzen können und immer vermehrt nutzen und auch intensiv nutzen. Wir haben auf der einen Seite die Cloud, die in der Schweiz gespeichert ist, **wir haben Sicherheitsvorkehrungen, die gewährleistet sind** und das alles mit der SIK abgesichert über Verträge.*

Der Antrag von GR Schulthess wurde mit 2 Ja-Stimmen gegen 20 Nein-Stimmen bei 17 Enthaltungen abgelehnt.

12) Kommt Stadtpräsident Niederberger auf seine Aussage *«dass die Sicherheit gewährleistet ist»* zurück?

Vielen Dank für eine zeitnahe Beantwortung dieser Fragestellungen.

Gemeinderat Georg Schulthess