Betreff: Weitere Informationen (Aktuelle Situation, IT-Sicherheit und Co.)

Sehr geehrte Damen und Herren,

die aktuelle Situation rund um das neuartige Coronavirus Covid-19 stellt uns alle vor große Herausforderungen. Für unsere Kommunen gilt es mögliche Quarantänemaßnahmen vorzubereiten und für eine große Anzahl von Mitarbeitern Notfall- bzw. Heimarbeitsplätze bereitzustellen. Bedingt durch die aktuelle Situation gibt es daher eine sehr große Nachfrage nach Heimarbeitsplätzen. Wie angekündigt, möchten wir Ihnen heute weitere Informationen zukommen lassen, wie die SIT in der derzeitigen Situation agiert und welche Maßnahmen wir planen. Gleichzeitig geben wir Rahmenbedingungen vor, die sich durch die z.T. unkontrollierte Nutzung von VPN-Verbindungen zwingend ergeben, um die bestehenden Lösungen stabil und für alle in gleichem Maße nutzbar betreiben zu können.

Wir planen, wie bereits angekündigt, weitere HomeOffice-Lösungen. Diese sollen auch auf privaten PCs verwendet werden können. Die heutigen und hier beschrieben Lösungen sind aus Sicherheitsgründen **nicht** für den Einsatz auf privaten Rechnern geeignet. Auch wenn wir das nicht verhindern können, weisen wir auf das große Risiko für Ihre eigenen System und für den Verband hin. Das Risiko für die System der SIT ist im Bereich der ehemaligen KDZ besonders hoch. Hierzu wird es morgen noch einmal eine gesonderte Mail geben, bei der wir auf den Einsatz dieser neuen Lösungen eingehen.

Zunächst folgen einige Sicherheitsregeln und Rahmenbedingungen, die sich u.a. aus Hinweisen der Vitako (https://www.vitako.de/Publikationen/PM_IT-Sicherheit%20unter%20Corona.pdf) ergeben.

Die Nutzung der seitens der SIT bisher angebotenen VPN-Lösungen von privaten Endgeräten ist und bleibt untersagt.

Die bisherigen Sicherheitskonzepte des Verbandes gehen immer davon aus, dass die Geräte der Obhut und Verantwortung der jeweiligen Verwaltung unterliegen und deshalb durch (zentrale) technische und/oder organisatorische Regularien (GPOs, Virenschutz, FW-Regeln, etc.) über ein Mindestmaß an Sicherheit verfügen. Das Risiko, das durch private Endgeräte auftritt, wird seitens der SIT für nicht tragbar erachtet. Wir weisen darauf hin, dass eine Abweichung von dieser Empfehlung laut Satzung der SIT Schadenersatzansprüche der Verbandsmitglieder und des selbst Verbandes auslösen können.

Private Endgeräte befinden sich dauerhaft und häufig in fremden ungesicherten Netzen und sind damit permanent dem Treiben diverser krimineller Akteure ausgesetzt. Eingenistete bzw. schlummernde Trojaner können nicht ausgeschlossen werden. Die Schäden, die durch z.B. einen einzigen Verschlüsselungstrojaner, der sich vielleicht schon lange auf einem privaten Endgerät befindet, in unserem Verbandsgebiet hervorrufen werden könnte, übersteigt in der derzeitigen Lage bei weitem den aktuellen Nutzen durch Zugriffsmöglichkeiten für Heimarbeiter/innen. Ein hervorgerufener Stillstand größerer Bereiche im Rechenzentrum bzw. Verband macht die Heimarbeiter schneller handlungsunfähig als die derzeitige Verbreitung des Corona-Virus. In diesen Tagen wird davon ausgegangen, dass Hacker Ihre Bemühungen in der Hoffnung verstärken, dass Sicherheit zugunsten pragmatischer Lösungen vernachlässigt wird.

Daher ist dies ganz wichtig: *Die Nutzung der seitens einiger Verbandsmitglieder eigenständig betriebener Remotelösungen unterliegt nach wie vor der Verantwortung des jeweiligen Verbandsmitgliedes und erfolgt ebenfalls auf eigene Gefahr und Haftung. Wir empfehlen diese Lösung nicht von privaten Endgeräten aus zu nutzen!*

Sie bekommen auch gleich noch eine separate Mail, bei der wir auf die Lösungen CiscoAnyConnect (südliche Verbandsmitglieder) und iWanHome (nördliche Verbandsmitglieder) eingehen. Außerdem möchten wir an dieser Stelle schon einmal auf unsere neue Hotline verweisen.

Unter der Nummer **0271 77345 222** erhalten Sie Hilfe zu den Themen:

- iWANHome
- CiscoAnyConnect
- ECOS Boot Sticks

Mit freundlichen Grüßen

Maray Paul