Initiative Sicherer Bürgerdialog

Webinar-Tag zu E-Mail-Verschlüsselung

[10.06.2021] Zum Webinar-Tag über die E-Mail-Verschlüsselung in öffentlichen Verwaltungen lädt am 17. Juni die Initiative Sicherer Bürgerdialog ein. Die kostenlose Veranstaltung adressiert den Auf- und Ausbau von Mail-Infrastrukturen, Verschlüsselungsverfahren sowie den Einsatz von Zertifikaten in Verwaltungen und Behörden.

Ihren zweiten Webinar-Tag richtet am 17. Juni 2021 die Initiative Sicherer Bürgerdialog aus. Wie das Unternehmen Net at Work mitteilt, hat die erste Auflage im Frühjahr 2021 (wir berichteten) große Resonanz erfahren. Die Veranstaltung im Juni stehe nun unter dem Titel „Sicherer Bürgerdialog mit E-Mail-Verschlüsselung“ und richte sich vorrangig an IT-Verantwortliche in den öffentlichen Verwaltungen. Ziel sei es, die öffentliche Verwaltung über die Notwendigkeit zur sicheren E-Mail-Kommunikation untereinander, aber auch mit den Bürgerinnen und Bürgern zu sensibilisieren. Entsprechend werde auf dem Webinar-Tag über die E-Mail-Verschlüsselung in öffentlichen Einrichtungen informiert. Fokus der kostenlosen Online-Veranstaltung liege auf dem Aus- und Aufbau von E-Mail-Infrastrukturen, auf Verschlüsselungsverfahren sowie dem Einsatz von Zertifikaten in Verwaltungen und Behörden. „Mit jeder Verwaltung, die sich mit dem Thema sichere Bürgerkommunikation auseinandersetzt, kommen wir unserem Ziel ein Stück näher: darauf aufmerksam zu machen, wie wichtig E-Mail-Verschlüsselung für die Vertraulichkeit beim Austausch sensibler, personenbezogener Daten ist und wie schnell und einfach öffentliche Einrichtungen E-Mail-Verschlüsselung einführen und damit den Datenschutzauflagen gerecht werden können“, sagt Stefan Cink, Business Unit Manager NoSpamProxy und E-Mail-Sicherheitsexperte bei Net at Work. Zum Auftakt wird am Webinar-Tag Horst Joepen von Net at Work die Initiative Sicherer Bürgerdialog vorstellen – eine Kooperation von Net at Work, dem Anbieter des E-Mail-Security-Gateways NoSpamProxy, sowie D-TRUST, einem Unternehmen der Bundesdruckerei (wir berichteten). Anschließend erläutere Henry Georges (M.I.S.) von der zentralen Ansprechstelle Cybercrime Hamburg beim LKA Hamburg aktuelle Gefahren der E-Mail-Kommunikation und wie die IT-Verantwortlichen ihre Einrichtung davor schützen können. Er klärt laut Net at Work über die Möglichkeiten der Verschlüsselung der digitalen Kommunikation auf und zeigt unter anderem, wie Cyber-Kriminelle mit den Betrugsmaschen CEO Fraud und BEC Fraud unter Verwendung falscher Identitäten zum Erfolg kommen. Auch das Thema Messenger und deren Verschlüsselung sowie die Frage, wie sicher die Kommunikation aus dem Homeoffice ist, seien Bestandteil des Vortrags. Im Folgevortrag stelle Michael Gröber, Senior Product Manager Certificates & Managed PKI von D-TRUST, die unterschiedlichen Arten von Zertifikaten zur E-Mail-Verschlüsselung und Signatur vor. Digitale Zertifikate spielen als Vertrauensanker eine zentrale Rolle in modernen IT-Infrastrukturen. Gröber veranschauliche den Weg der Beantragung und Validierung von Zertifikaten innerhalb der Managed PKI Lösung CSM sowie die Vorteile der Nutzung einer Managed PKI im Zusammenspiel mit einer E-Mail-Gateway-Lösung. Zum Abschluss demonstriere Stefan Cink in seinem Vortrag „Verschlüsselter E-Mail-Versand als Behördenstandard – automatisiert und einfach“, warum die Gateway-basierte Verschlüsselung die beste Lösung für Behörden ist und räume mit Mythen im Kontext von Ende-zu-Ende-Verschlüsselung und EU-DSGVO auf.

(ve)

Weitere Informationen und Anmeldung

Stichwörter: IT-Sicherheit, Initiative Sicherer Bürgerdialog, D-TRUST, E-Mail-Verschlüsselung, Secure E-Mail, Gateway, Anti-Virus, Anti-Spam, Anti-Malware