

E-Mail-Kommunikation

Guter Schutz im Hintergrund

[20.10.2022] Kommunen tragen eine besondere Verantwortung für den Umgang mit den Daten von Bürgerinnen und Bürgern. Ein Gespräch über sichere E-Mail-Kommunikation mit Stefan Cink vom Lösungsanbieter Net at Work und Peter Sedlmayr vom Serviceprovider LivingData.

Herr Cink, Herr Sedlmayr, warum ist E-Mail-Sicherheit und -Vertraulichkeit für Kommunen aktueller als je zuvor?

Peter Sedlmayr: Immer mehr Behördengänge werden digital erledigt, und eine sichere E-Mail-Kommunikation gehört dazu. Man muss als Bürger darauf vertrauen können, dass die digitale Kommunikation mit einer Behörde sicher ist und die persönlichen Daten auch nur von den berechtigten Personen verarbeitet werden. Eine sichere Kommunikation schafft Vertrauen und gehört zu einer modernen Verwaltung.

Stefan Cink: Das Bundeskriminalamt hat in seinem Lagebild Cybercrime im Mai eindringlich geschildert, dass die kommunalen Verwaltungen in Deutschland zunehmend Ziel von Cyber-Attacken sind. Ungesicherte E-Mail-Kommunikation ist dabei nach wie vor eines der Haupteinfallstore für gefährliche Schad-Software. Ausgeklügelte Phishing-Attacken und Social-Engineering-Kampagnen versuchen mit gefälschten E-Mails Zugangsdaten zu stehlen oder ungewollte Vorgänge auszulösen. Kommunen müssen hier als Teil der Kritischen Infrastruktur mit gutem Beispiel vorangehen. Die Verantwortlichen haben zudem größtes Interesse daran, den mit einem Hacking einhergehenden Schaden, Reputationsverlust und Ärger zu vermeiden.

Woran können Kommunen gute E-Mail-Security-Lösungen erkennen?

Cink: Im Kern geht es um zwei Aspekte: die Leistungsfähigkeit des Produkts und die Einfachheit der Nutzung. Für die Bewertung der Leistungsfähigkeit gibt es zahlreiche unabhängige Tests und Rankings wie beispielsweise den VBSpam+ Award des Virus Bulletin oder das TechConsult Professional User Ranking E-Mail Security. Gute Lösungen sorgen mit selbstlernenden Verfahren, dem Verzicht auf umständliche Quarantäne-Ordner und automatisierter Zertifikatsverwaltung für geringe Aufwände bei der Einführung und Administration. Die intensive Nutzung von Reputationsverfahren sowie eine cloudbasierte, übergreifende Erkennung von neuen Angriffen sorgen für höchstmöglichen Schutz.

Sedlmayr: Bei der Einfachheit der Nutzung überzeugen gatewaybasierte Lösungen. Dabei werden der Schutz vor Angriffen und auch die Verschlüsselung von E-Mails an einer zentralen Stelle organisiert und umgesetzt. Durch die selbstlernenden Fähigkeiten guter Lösungen, passen sie sich ständig an wechselnde Kommunikationspartner und Gegebenheiten an. Als Managed Service kann eine solche Lösung für E-Mail-Sicherheit in wenigen Tagen umgesetzt werden.

„Ungesicherte E-Mail-Kommunikation ist eines der Haupteinfallstore für gefährliche Schad-Software.“
Welche Rolle spielt die E-Mail-Verschlüsselung dabei?

Cink: Die vollständige Verschlüsselung von E-Mail-Kommunikation sollte für jede Verwaltung selbstverständlich sein, ist sie doch Bestandteil des vom Bundesamt für Sicherheit in der

Informationstechnik empfohlenen Grundschutzes. Jede unverschlüsselt gesendete E-Mail ist ebenso vertraulich wie eine Postkarte. So kann man als Verwaltung mit den persönlichen Daten von Bürgerinnen und Bürgern nicht umgehen.

Sedlmayr: Als Empfänger einer verschlüsselten Mail kann man zudem mit der digitalen Signatur prüfen, ob eine Nachricht auch wirklich von dem Mitarbeiter der Verwaltung kommt. Somit müssen in der digitalen Kommunikation zwischen Bürger und Behörde oder der Behörden untereinander keine Kompromisse eingegangen werden.

Was empfehlen Sie den Kommunen?

Cink: Für den Wettlauf mit den immer professioneller agierenden Angreifern braucht es tiefes Security-Know-how, das in der Verwaltung meist nicht vorhanden ist. Statt das Thema aus Ressourcenmangel auf die lange Bank zu schieben, sollten Kommunen es kurzfristig auslagern und in die Hände externer Experten legen.

Sedlmayr: Wir haben zusammen mit der AKDB unter dem Produktnamen NextGO ein modulares Managed-Services-Angebot geschaffen, das es erlaubt, den IT-Betrieb von Kommunen schnell zu modernisieren und flexibel zu gestalten. Sogar ein vollständiges Outsourcing der gesamten IT in die AKDB-Cloud ist möglich. E-Mail-Sicherheit gehört dabei zu den besonders oft ausgelagerten Bereichen; und wir nutzen dafür NoSpamProxy von Net at Work. Neben dem Managed Service bieten wir auch die Einrichtung und Integration des Mail Security Gateways in die bestehenden Infrastrukturen an.

Das klingt fast zu einfach, um wahr zu sein. Wo ist der Haken?

Cink: Die technischen Verfahren im Hintergrund sind natürlich immer noch sehr komplex und erfordern tiefes Know-how aufseiten der Hersteller, aber für die Kommunalverwaltung ist es mit modernen Lösungen und Managed Services wirklich einfach. Früher hatte E-Mail-Verschlüsselung zu Recht den Ruf, kompliziert und wenig nutzerfreundlich zu sein. Das hat sich mit den neuen Lösungen komplett gewandelt. Heute werden guter Schutz und höchste Vertraulichkeit bei der E-Mail-Kommunikation einfach im Hintergrund organisiert – ohne dass die Nutzenden es überhaupt merken müssen. E-Mail-Sicherheit ist einfach, man muss es nur machen.

()

Dieses Interview ist in der Ausgabe Oktober 2022 von Kommune21 im Schwerpunkt IT-Sicherheit erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Datenschutz, LivingData, E-Mail-Sicherheit