Effiziente und sichere Behördenkommunikation

Am Institut für Internet-Sicherheit – if(is) wurde im Rahmen eines wissenschaftlichen Projekts eine innovative Kommunikationsplattform namens „Quvert" konzipiert und entwickelt. Ausgehend von der Idee, das Kommunikationsverhalten von Jugendlichen auf den Businesskontext zu übertragen, wurde ein erster Prototyp umgesetzt und getestet.

Im Arbeitsalltag bekommt Information eine nie zuvor dagewesene Wichtigkeit. Die richtigen Informationen schnell zur Verfügung zu haben, macht die Arbeit einfacher, besser und schneller. Und: Es war noch nie einfacher als heute, Informationen, Erkenntnisse, Erfahrungen und Wissen in einem Bruchteil von Sekunden mit Kollegen, Partnern oder Bürgern zu teilen. Durch digitale Kommunikation und das Internet ist es möglich geworden, dass jeder Mensch unabhängig von seinem sozialen Status an der globalen Kommunikation aktiv teilnehmen kann.

Diese Kommunikation kann ganz unterschiedlich ablaufen und verschiedene Grade der Effektivität erreichen. Sie kann in einem geschützten oder ungeschützten Kommunikationssystem stattfinden. Sie kann uni- bis multidirektional sein. Letztendlich ist Kommunikation ein komplexes System, das hauptsächlich aus protokollspezifischen, technischen und menschlichen Komponenten besteht.

Insbesondere im Öffentlichen Dienst ist ein effizientes, smartes und sicheres Kommunikationswerkzeug von essentieller Wichtigkeit im Zuge der immer weiter fortschreitenden Digitalisierung, die auch vor öffentlichen Instanzen keinen Halt macht. Insbesondere Kosten spielen im Öffentlichen Dienst oftmals eine große Rolle. Die zu entwerfenden Werkzeuge sollten also möglichst günstig in Anschaffung und Unterhalt sein, müssen aber ein maximales Maß an Nutzbarkeit, Sicherheit und Schutz von persönlichen Daten mitbringen. Insbesondere innerhalb der öffentlichen Verwaltungen kommt es zur Erhebung und Verarbeitung von personenbezogenen und vertraulichen Daten. Der Bürger muss sich sicher sein, dass die Daten nicht an Dritte weitergegeben werden und er die Hoheit über seine Daten behält. Selbstbestimmung muss durchsetzbar sein, und es müssen Datenschutz und Datensicherheit in hohem Maße „by Design" umgesetzt werden. Ebenfalls von bedeutender Wichtigkeit ist es, Behördenprozesse und Workflows digital abbildbar zu machen, damit es beispielsweise zu einer Verkürzung von Bearbeitungszeiten kommt. Davon profitieren Kunden und Behörden. Für Mitarbeiter im Öffentlichen Dienst muss das Kommunikationswerkzeug intuitiv nutzbar sein, und es muss deren Arbeitsalltag effektiver gestalten, damit es akzeptiert und effektiv genutzt wird.

Kommunikationsformen

Wieso ist Kommunikation auch für den Öffentlichen Dienst von so essentieller Wichtigkeit? Wie oben bereits erläutert, ist Kommunikation ein Prozess, der dem Ziel dient, Informationen auszutauschen, die das Arbeiten erleichtern sollen. Fach- und Füh-

rungskräfte verbringen den größten Anteil ihrer Arbeitszeit mit Kommunikation. Die Effizienz dieser Kommunikation orientiert sich an der Kommunikationsstruktur sowie an den individuellen Fähigkeiten der jeweiligen Person. Die Kommunikation lässt sich auch klassifizieren, etwa in dienstweggebunde oder ungebundenene, rein interne oder organisationsübergreifende, formelle oder informelle sowie Individual- oder Massenkommunikation. Für all diese Formen bietet sich die moderne chatbasierte Kommunikation an. Dadurch können einzelne Anforderungen bedient und teilweise sogar kombiniert werden.

Durch die Einführung eines Chat-Systems, in dem alle Mitarbeiter gleich verbunden sind, können Hierarchien ein Stück weit verflacht werden, sodass alle Teilnehmer eines Kommunikationssystems auf einer Kommunikationsebene stehen und Grenzen der Hierarchie verschwimmen. Die Arbeit flexibilisiert sich hinsichtlich Ort, Zeit, Struktur und Zusammenarbeitsform, wodurch der Grad an Effektivität innerhalb einer öffentlichen Stelle steigt. Die Kommunikationsbeziehung verändert sich also von vertikalen Hierarchieebenen hin zu einer horizontalen, in der Kommunikation auf der gleichen Ebene effektiv stattfindet. Für Genehmigungen oder verbindliche Prozesse kann die vertikale hierarchische Struktur allerdings im Kommunikationssystem ebenfalls abgebildet werden. Es ist sogar möglich und sinnvoll, Nichtabstreitbarkeit in einem modernen Kommunikationssystem zu implementieren respektive einen rechtsverbindlichen Nachweis möglich zu machen.

Neben all den technischen und unternehmerischen Vorteilen, die durch ein solches modernes Kommunikationswerkzeug entstehen, kann die Kommunikationsplattform auch als soziales Tool verstanden werden. Dies ist allerdings nicht die Kommunikationsplattform an sich, sondern die Kommunikationsplattform muss Möglichkeiten und Funktionen bieten, mit anderen Personen über zu definierende Kanäle in Verbindung zu treten. Dadurch lässt sich in einem nächsten Schritt auch kollaboratives Arbeiten einfach umsetzen. Es lassen sich Interaktionen herbeiführen, die Rückkopplungen für Selbstorganisation ermöglichen und „Incentives" erlauben. Diese Kommunikationskanäle lassen sich im Sinne eines offenen, transparenten und vernetzten, also eines digitalisierten Verwaltungsapparats verstehen.

Von Grund auf sicher (IT-Security by Design)

Das Austauschen von Informationen und das Thema IT-Sicherheit gehen heutzutage miteinander einher. Chatbasierte Anwendungen ohne entsprechende kryptographische und vertrauenswürdige Absicherung können durchsichtig für Dritte sein und geraten dadurch schnell in Verruf. Gerade bei Anwendungen ausländischer Anbieter kann der Datenfluss die Grenzen Deutschlands und Europas überqueren, wodurch dieser dem Datenschutzrecht und der Politik des entsprechenden Landes unterzuordnen ist. Ebenso lässt die Verwendung von durch Dritte angebotenen Diensten und das zwangsläufig damit verbundene ungewollte Teilen von Informationen den Anwender selbst zum Produkt werden. Gerade an Stellen, wo personenbezogene Daten zusammenlaufen und auch verarbeitet werden, ist die Entscheidung für einen solchen Dienst fatal. Die Hoheit über die eigenen Daten muss folglich in den Händen des jeweiligen Besitzers liegen. Dementsprechend ist neben den bereits genannten Anforderungen an eine moderne Kommunikationsplattform die Absicherung der ausgetauschten Daten auf technischer, allerdings auch auf Ebene des Benutzers, von Bedeutung und somit die IT-Sicherheit als essentieller Faktor aufzugreifen.

„IT-Security by Design" ist dabei das Stichwort und muss bei der Planung einer modernen und fortschrittlichen Kommunikationsplattform berücksichtigt werden. Dies gilt nicht nur für die Transportwege der Daten. Die Serverkomponenten sowie die Clientseite müssen von Beginn an die IT-Sicherheit einverleibt bekommen. Eine Ende-zu-Ende-Verschlüsselung schafft dabei das nötige Vertrauen und schließt Dritte vollständig aus, die Verifikation der Identität und die Authentifizierung aller Anwender garantieren die Echtheit und Glaubwürdigkeit eines Gegenübers und die langfristige Archivierung von bestimmten Nachrichten ermöglicht die Nachweisbarkeit von Prozessen.

Das E-Mail-System als mittlerweile alteingesessenes Kommunikationswerkzeug ist aus technischer Sicht vergleichsweise unsicher. Das Manipulieren von ganzen Nachrichten oder das Fälschen des Absenders stellt heutzutage keine technische Herausforderung mehr dar. Möglichkeiten zur Verschlüsselung ganzer Nachrichten existieren bereits seit mehr als 20 Jahren, sind allerdings nicht „Out-of-the-box" einsetzbar. Geschuldet ihrer Komplexität und nicht vorhandener Benutzerfreundlichkeit finden die Lösungen nur wenig Anklang bei Anwendern sowie IT-Verantwortlichen.

Moderne Kommunikation – effizient, sicher und nutzbar

Im aktuellen Informationszeitalter wächst neben der steigenden Bedeutung der Information auch deren Menge. Oftmals vergehen Stunden, ehe das Ende der abzuarbeitenden E-Mail-Flut zu erkennen ist. Demzufolge ist es umso wichtiger, neben den bereits erwähnten Eigenschaften, die Effizienz der Übermittlung der eigentlichen Information zu steigern. So verbrauchen die Mitarbeiter heutzutage sehr viel Zeit, um den eigentlichen Inhalt einer E-Mail zu erkennen. Die einzelnen E-Mails enthalten sehr viele Formalitäten, wie die persönliche Anrede des schon ohnehin seit Dekaden bekannten Kollegen, die sich doch oft wiederholenden Grußformeln bis hin zur sperrigen Signatur. Die eigentlich relevante Information ist oftmals irgendwo dazwischen zu entdecken.

Die chatbasierte Kommunikation hakt genau hier ein. Am Beispiel der auf Smartphones verwendeten Chat-Anwendungen, die sich mittlerweile auch mit der zugehörigen Desktopanwendung verbinden und synchronisieren lassen, ist die mögliche Steigerung der Effizienz bei der Übermittlung von Informationen zu erkennen. Formalitäten finden selten ihren Weg in einen solchen Chat und Fragestellungen lassen sind nicht selten symbolisch beantworten. Die Informationsflut kann hierdurch gerade bei der internen Kommunikation öffentlicher Instanzen reduziert und weitestgehend optimiert werden.

Diese Problematik, genauso wie die bereits gezeigten Angriffsvektoren, lässt sich mit einer innovativen Kommunikationsplattform aus dem Weg räumen. Unser Prototyp „Quvert" wurde konzeptionell genau auf diese Herausforderungen zugeschnitten. Neben der von Anfang an bedachten IT-Sicherheit und der Optimierung des Kommunikationsverhaltens bildet die Benutzerfreundlichkeit die dritte Säule des

Fundaments unserer innovativen und modernen Kommunikationsplattform. Zum Schutz vertrauenswürdiger Kommunikation und zur Wahrung der Privatsphäre beinhaltet Quvert ein integriertes, robustes, auf Standards basierendes Verschlüsselungssystem, das nur an wenigen Schnittstellen mit dem Benutzer in Berührung kommt – ganz im Sinne der Benutzerfreundlichkeit, die heute noch bei vielen anderen IT-Sicherheitsprodukten vernachlässigt wird und die Anwender massiv in der Nutzung von Sicherheitslösungen eingeschränkt und behindert. Das Paradebeispiel unzureichender Benutzerfreundlichkeit zeigt die E-Mail-Verschlüsselung, die lediglich durch die Verwendung zusätzlicher Software zur Option wird. Dabei müssen zum verwendeten E-Mail-Client oftmals noch Programme und Add-ons installiert und konfiguriert sowie Schlüssel erzeugt und kompliziert ausgetauscht werden. Ohne fortgeschrittene Kenntnisse in den Bereichen der Computersoftware und im Schlüsselmanagement sind die nötigen Schritte von Laien kaum durchzuführen. Quvert setzt daher zur Absicherung der Kommunikation auf etablierte und vertrauenswürdige IT-Sicherheitstechniken und lässt dabei den Benutzer diese Features nur passiv nutzen.

Zusammenfassend lässt sich für Quvert festhalten: Die IT-Sicherheit wurde bereits in der Konzeptionsphase, also direkt von Beginn an, berücksichtigt (Security by Design) sowie im Sinne der Nutzbarkeit für den Anwender weitestgehend transparent gestaltet. Des Weiteren nimmt die Lösung neue Herausforderungen an und macht die Hoheit der im Kontext des Informationsaustauschs anfallenden Daten zum Thema. Dazu verfolgt Quvert den Ansatz, die zur Vermittlung der Nachrichten benötigten Server in die Hände der jeweiligen Instanz zu geben und diese in den jeweiligen Dienststellen zu betreiben. Ganz nach dem Motto: Ihre Server, Ihre Mitarbeiter, Ihre Daten. In weiteren Schritten adressiert Quvert eine organisationsübergreifende Kommunikation, und das mit derselben Maßgabe an IT-Sicherheit und Authentizität der Nutzer. Erste Konzepte für eine solche Erweiterung der Kommunikationsplattform existieren bereits und verfolgen den Ansatz, verschiedene Stellen miteinander zu vernetzen und die Kommunikation auch übergreifend auf beschriebene Art und Weise effizienter, sicherer und benutzerfreundlicher zu gestalten.

Featurettes

Neben all den bereits beschriebenen Aspekten und Anforderungen ist natürlich auch die Entwicklung von Features und neuen Ideen essentiell für den Erfolg eines modernen Kommunikationssystems. Die Chat-Kommunikation ist eine Basisfunktion von Quvert. Um sich an die Individualität, Flexibilität und Größe von Behörden anzupassen, müssen deutlich mehr Innovationen in der Chat-Applikation realisiert werden. Möchte ein Sachbearbeiter beispielsweise eine Freigabe für einen Vorgang beantragen, muss er heutzutage E-Mails versenden oder Formulare ausfüllen. Dies kostet Zeit und Ressourcen, die eigentlich besser zu nutzen wären. Die Kommunikationsplattform bietet eine „Handshake"-Funktion, die solche Freigabeprozesse digitalisiert abbilden kann. Die Anfrage zur Freigabe wird an den entsprechenden Vorgesetzten versendet, der eine binäre Entscheidung treffen kann: „Freigeben" und „Ablehnen". Es wird technisch und kryptographisch sichergestellt, dass diese Entscheidung hinterlegt wird, und im Streitfall kann eine solche Freigabe nach dem Mehraugenprinzip dechiffriert werden und somit ist eine Absprache nicht abstreitbar, sollte ein Gerät nicht auffindbar sein oder ausgetauscht worden sein.

Abb. 1: Handshake für verbindliche Arbeitsabläufe

Weiterhin ist es wünschenswert, die gängige Funktion „Status", die aus anderen Chat-Systemen bekannt ist, prominenter zu gestalten und mit sinnvollen Funktionen zu erweitern. Beispielsweise mit einem temporär setzbaren Status, beispielsweise „Bahnfahrt", um mit allen Kontakten in einer Behörde zu teilen, dass die Erreichbarkeit momentan stark eingeschränkt ist. Nach Ablauf der definierten Dauer wird der Status automatisch auf den vorherigen dauerhaften Status zurückgesetzt.

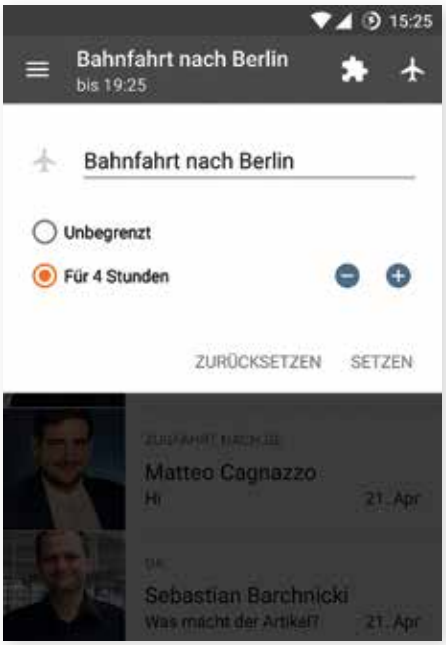

Abb. 2: Anzeige des Verfügbarkeitsstatus

Quvert bietet weiterhin die Möglichkeit, Mitarbeiter mit Kompetenz-„Tags" auszustatten. Diese bilden die Kompetenzen der einzelnen Mitarbeiter ab. Dadurch können Hard und Soft Skills innerhalb einer Organisation strukturiert und für Kollegen sichtbar gemacht werden. Sucht ein Mitarbeiter beispielsweise Hilfe bei Excel-Tabellen, besteht die Möglichkeit, dass er nach „Excel" sucht und direkt alle Mitarbeiter und Kontaktinformationen angezeigt bekommt, um Hilfe zu bekommen. Diese einzelnen „Tags" lassen sich zu einem Netzwerk zusammenfassen, um eine „Kompetenzlandkarte" zu generieren. Diese kann beispielsweise den Bedarf an Kompetenzen heute und morgen visualisieren und bei Entscheidungen bezüglich Einstellungen von Mitarbeitern helfen. Insbesondere Mitarbeiter, die sich neben der Arbeit weiterqualifizieren oder ein breitgefächertes Wissensspektrum haben, haben somit eine erhöhte Chance, bei Personalentscheidungen intern berufen zu

werden. Weitere Möglichkeiten, um Nutzen aus der Analyse von solchen Kompetenznetzwerken zu ziehen, werden momentan erforscht.

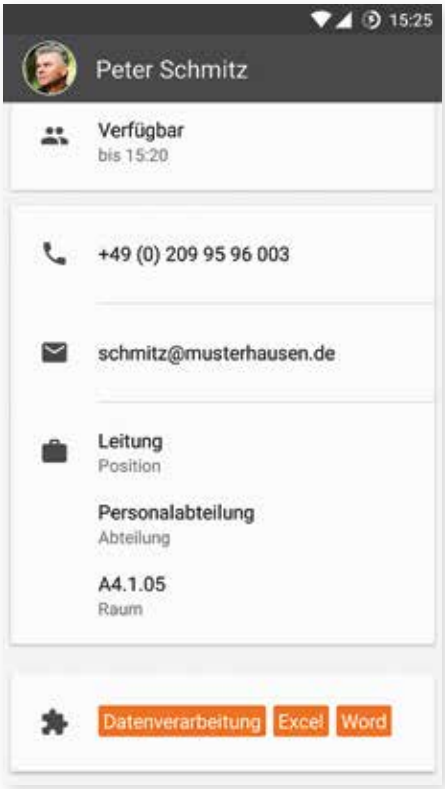

Abb. 3: Darstellung von Kompetenzen

Mit der Darstellung von Kompetenzen lässt sich eine weitere, für soziale Netzwerke typische Funktion etablieren, nämlich Kanäle. Innerhalb eines Kanals kann ein beliebiger Nutzer eine Frage zu einem bestimmten Themengebiet stellen. Diese kann dann in Form eines offenen Forums diskutiert und gelöst werden. Ein Vorteil, der durch dieses Feature entsteht, ist, dass das Unternehmen im Zuge eines transparenten, offenen Unternehmens einzelne Diskussionen veröffentlichen kann und somit den Kunden näher an die Entwicklungsarbeit heranlässt. Ein weiterer Vorteil, der durch Kanäle impliziert wird, ist, dass Mitarbeiter ihr Wissen konservieren und Fragestellungen außerhalb ihres normalen Tagesgeschäfts beantworten können, um dieses etwas variabler zu gestalten.

Weitere Aspekte

Zurzeit arbeiten wir an weiteren Aspekten, die helfen sollen, das Kommunikationssystem Quvert einfach und sicher nutzen zu können. Neben der Chat Kommunikationen soll es auch möglich sein, Voice-Nachrichten verschlüsselt zu übertragen, um unkompliziert Informationen auszutauschen. Falls der Empfänger in einer Besprechung sitzt und diese noch abhören kann, er aber erkennen möchte, ob die Voice-Nachricht wichtig oder dringlich ist, kann er diese in Text umwandeln, um den Inhalt zu lesen.

Ein weiteres Forschungsthema ist die Minimierung der Lesbarkeit durch andere, die zum Beispiel im Zug, im Flugzeug oder in einer Besprechung neben einem sitzen. Hier soll sichergestellt werden, dass sensible Informationen nicht durch Dritte gelesen werden können.

Fazit

Kommunikation im Öffentlichen Dienst ist ein essentieller Bestandteil für die Produktivität und die Zufriedenheit der Bürger. Nur effizient kommunizierende Dienststellen werden sich im Zuge der Innovationskraft der Digitalisierung erfolgreich darstellen können und einen echten Mehrwert für Bürger, durch beispielsweise kürzere Bearbeitungszeiten, bieten. Die Mitarbeiter in Behörden haben die Möglichkeit, schnell, flexibel und stressfrei intern zu kommunizieren und mehr Zeit und Ruhe für die Vorsprachen der Bürger zu gewinnen. Dadurch werden Abstimmungsgespräche und Freigaben nur noch Mittel zum Zweck und die kostbare Zeit kann effizient genutzt werden. Es kommt im Allgemeinen zu einer Neuorganisation der Arbeit. Gerade jüngere Generationen können das innovative Konzept, das auf der Instant-Messaging-Funktion aufbaut, schnell adaptieren und effizient einsetzen.

Für den Öffentlichen Dienst ist es von hoher Wichtigkeit, den kulturellen Wandel zur digitalisierten Welt mitzugehen. Kernfaktoren für Öffentliche Verwaltungen sind die Optimierung und die Digitalisierung von Prozessen und Workflows. Wenn alles um uns herum sofort und immer verfügbar ist, aber ein Passantrag beim Bürgeramt 6 Wochen dauert, wird das für eine zunehmende Polarisierung bei der Bürgerschaft und langfristig vermutlich für Unbehagen sorgen. Im Allgemeinen lässt sich festhalten, dass die Personalarbeit, deren wichtigster Bestandteil die Kommunikation ist, durch die Digitalisierung einen Kulturwandel erfährt. An der Stärkung technischer und sozialer Innovationen führt kein Weg vorbei, auch nicht im Öffentlichen Dienst.

Aus diesem Grund wurde Quvert als ein Werkzeug für effiziente und sichere Kommunikation, zum Beispiel in Behörden, entwickelt. Für weitere Informationen oder eventuelle Partnerschaften besteht die Möglichkeit, mit dem Projektteam direkt in Kontakt zu treten (siehe www.quvert.de). Weiterhin sind wir sehr an Ihrem Feedback interessiert und für Kommentare, Kritik und Lob jederzeit offen. ■

MATTEO CAGNAZZO
ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und leitet den Forschungsbereich Gesundheitswesen.

NORBERT POHLMANN
ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT.

PATRICK WEGNER
ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und leitet den Forschungsbereich IT-Sicherheits-Apps.