



Kein E-Government ohne IT-Sicherheit

Ob Sicherheitslücken wie Lock4j, installierte Schadprogramme oder Phishing-Mails – mittlerweile gibt es zahlreiche Methoden, mit denen Kriminelle versuchen, sich Zugang zu sensiblen Daten zu verschaffen. Cyberattacken sind auf dem Vormarsch und werden mit Fortschreiten der Digitalisierung immer raffinierter. Besonders die kommunale Verwaltung ist zu einem beliebten Ziel für Angriffe geworden, wie mehrere Vorfälle in den vergangenen Monaten zeigten. Die Folgen sind immens: Stillgelegte Behörden, Schäden in Millionenhöhe und veröffentlichte Datensätze. Viele Kommunen sind gegen solche Attacken nicht ausreichend geschützt.

Die im Februar stattgefundenene Online-Veranstaltungsreihe »Digital.Kommunal.Sicher – Informationssicherheit in der Kommunalverwaltung« der kommunalen Spitzenverbände und des Dachverbands kommunaler IT-Dienstleister (KDN) hatte zum Ziel, auf Gefahren im digitalen Raum aufmerksam zu machen und für die IT-Sicherheit in nordrhein-westfälischen Städten, Kreisen und Gemeinden zu sensibilisieren. Auf der Agenda standen qualifizierte Referentinnen und Referenten, die ihre Expertise und Know-how zur Vermeidung von IT-Sicherheitsvorfällen im kommunalen Umfeld teilten. Rund 1.000 Teilnehmende aus der Verwaltung, von Mitarbeitenden bis hin zu kommunalen Spitzenbeamt*in-



nen, nahmen an den insgesamt vier Terminen teil.

Cyberangriffe: Je kleiner, desto verwundbarer?

Höhepunkt der Veranstaltungen war eine Live-Berichterstattung der Stadt Witten. Kommunalvertreter berichteten offen über ihre Erfahrungen als Opfer eines Cyberangriffes auf die Verwaltung im Oktober 2021 – von der Erstreaktion nach dem Angriff bis hin zur Organisation des Wiederaufbaus. »Durch den Angriff waren die städtischen Systeme der Stadt Witten massiv eingeschränkt. Wir waren weder per E-Mail noch telefonisch zu erreichen. Die IT-Systeme der Stadtverwaltung gingen komplett in die Knie und waren nicht nutzbar«, berichtete IT-Leiter Andreas Hasenberg, Stadt Witten.

Am Beispiel der Stadt Witten zeigt sich, dass insbesondere Bürgerinnen und Bürger die Opfer eines Hackerangriffs sind: Zunächst, indem sie städtische Dienstleistungen nur eingeschränkt nutzen können. Und im Einzelnen auch durch die Veröffentlichung von privaten Daten.

Cyberangriffe wie diese nehmen zu. Viele Gemeinden, Städte und Landkreise waren bereits ebenso betroffen wie kommunale Einrichtungen. Dabei geht es meist um gezielte Destabilisierung, Angriffe auf die Verfügbarkeit kommunaler IT und um digitale Erpressung mittels Ransomware.



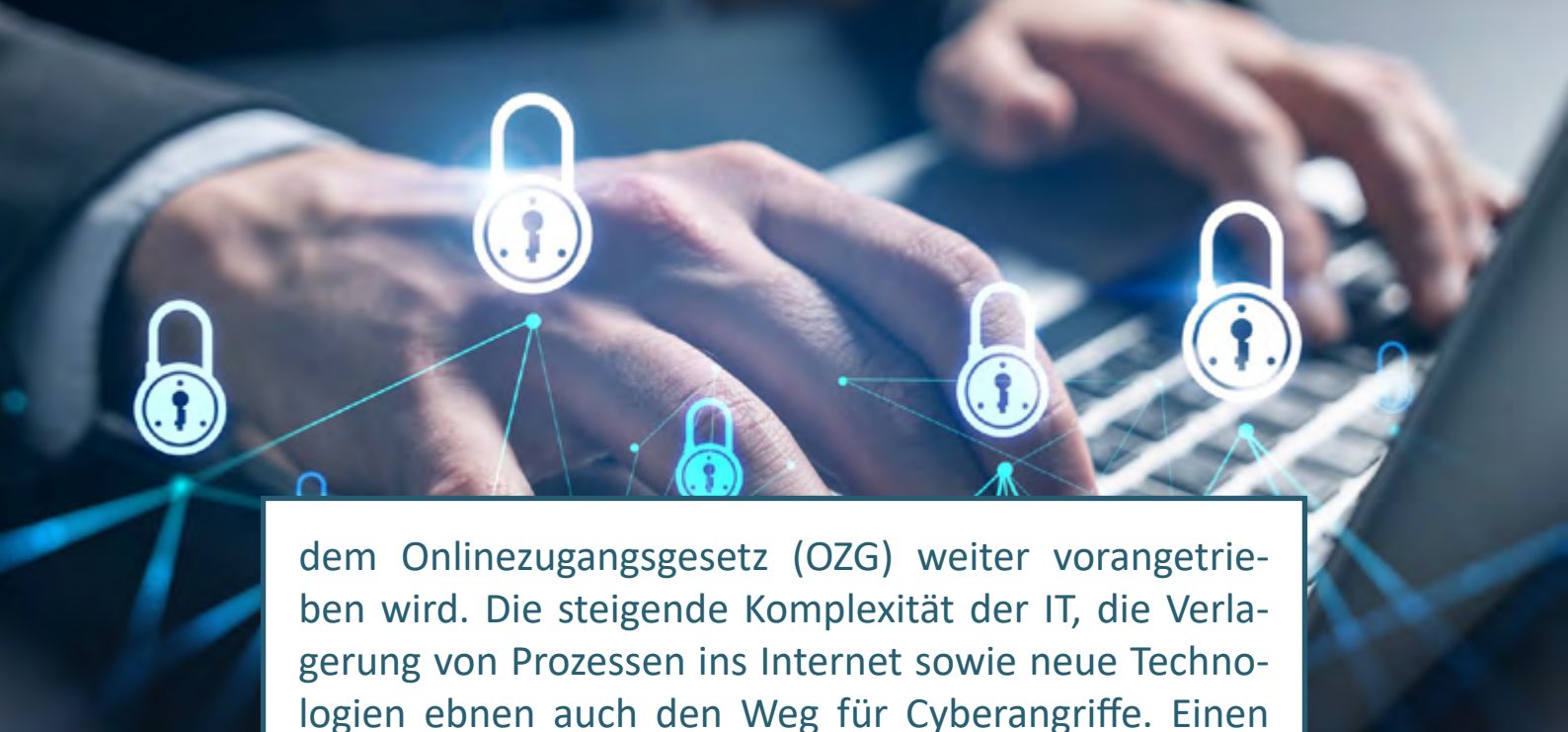
Faktor Mensch: Unterschätzte Sicherheitslücke?

Neben Fragen wie »Wer haftet bei einem Hackerangriff« oder »Was passiert, wenn ein IT-Sicherheitsfall eintritt?« wurde der Fokus auch auf die sechzig Zentimeter vor dem Bildschirm, dem Menschen, gelegt. Nicht nur die IT muss auf dem aktuellsten Stand sein. Weiter sollten Mitarbeitende geschult und für die unterschiedlichen Formen von Cyberbedrohungen sensibilisiert werden. Eine wichtige Rolle spielt hierbei die Früherkennung.

NRW stärkt Cybersicherheit in den Kommunen

Parallel zur Veranstaltung ist der Warn- und Informationsdienst für Kommunen »KWID« unter Beteiligung der Landesregierung NRW, der kommunalen Spitzenverbände und des KDN gestartet. Dr. Frank Laicher, Chief Information Security Officer der Landesregierung NRW, stellte den neuen Dienst vor: »Ein Rauchmelder klingelt erst, wenn der Brand schon im Gange ist. Wie toll wäre es, wenn ein Warnsystem schon vor dem Eintreten eines Sicherheitsvorfalls benachrichtigt?« Mit dem KWID können Städte und Gemeinden in NRW kostenfrei sämtliche IT-Sicherheitshinweise abrufen, die auch die Landesverwaltung selbst erhält. So wird ein Beitrag zur Sicherheit der Infrastruktur geleistet.

Die Informationssicherheit in der Kommunalverwaltung nimmt einen besonderen Stellenwert ein, nicht zuletzt, weil die Digitalisierung aller Verwaltungsleistungen mit



dem Onlinezugangsgesetz (OZG) weiter vorangetrieben wird. Die steigende Komplexität der IT, die Verlagerung von Prozessen ins Internet sowie neue Technologien ebnen auch den Weg für Cyberangriffe. Einen hundertprozentigen Schutz vor Cyberattacken gibt es nicht, dennoch lassen sich viele Risiken mithilfe von organisatorischen und technischen Maßnahmen deutlich verringern, lautet das Resümee der Expertinnen und Experten.

Ab sofort stehen Ihnen die Präsentationen sowie ein Videomitschnitt der Veranstaltungsreihe »Digital.Kommunal.Sicher« über die [Webseite des KDN](#) zur Verfügung.

Zur Autorin

Sarah Dobrowolski arbeitet seit Juni 2020 als Beraterin für Kommunikation und Marketing im Kompetenzzentrum Digitalisierung des KDN. In dieser Funktion betreut Sie die Medienkanäle des Dachverbandes und entwickelt crossmediale Kommunikations- und Informationskampagnen im Bereich der Verwaltungsdigitalisierung. Als gelernte Technik- und Innovationsjournalistin hat Sie bereits mehrjährige Erfahrungen in der Konzeption, Planung und Durchführung interner wie externer Kommunikationsmaßnahmen.

