Stadt Braunschweig
Der Oberbürgermeister

20-14935-01
Stellungnahme
öffentlich

Betreff:
IT-Sicherheit

Organisationseinheit:	*Datum:*
Dezernat II 10 Fachbereich Zentrale Dienste	27.01.2021

Beratungsfolge	*Sitzungstermin*	*Status*
Finanz- und Personalausschuss (zur Kenntnis)	29.01.2021	Ö

Sachverhalt:

Zunächst möchte ich darauf hinweisen, dass die Stadt Braunschweig und ihre Gesellschaften jeweils eigenständig für ihre IT-Sicherheit zuständig sind soweit sie ihre IT-Systeme eigenständig betreiben. Die nachfolgenden Ausführungen beziehen sich auf die IT-Sicherheit bei der Stadtverwaltung sowie den von ihr mit IT-Leistungen versorgten Gesellschaften. Dabei handelt es sich um die Braunschweig Stadtmarketing GmbH, die Braunschweig Zukunft GmbH und die Grundstücksgesellschaft Braunschweig mbH.

Die Beantwortung der Anfrage durch die anderen städtischen Gesellschaften ist in der Anlage aufgeführt.

Die Stadt Braunschweig wird durch das Niedersächsische Computer Emergency Response Team (N-CERT) im Nds. Ministerium für Inneres und Sport seit dem Jahr 2016 zur IT-Sicherheit und Cybersicherheit beraten und betreut. Ein repräsentatives monatliches IT-Sicherheitslagebild wird seit 2,5 Jahren erstellt und gibt einen guten Einblick in die globale Bedrohungslage mit Bezug zur Landes- und Kommunalverwaltung in Niedersachsen.

Im IT-Sicherheitslagebild des Nds. Ministerium für Inneres und Sport für den Monat November 2020 wird die Bedrohung für die Landesverwaltung und Kommunalverwaltung durch Schadsoftware und Cyberangriffe weiter als erhöht eingestuft. Angreifende versuchen zudem weiter, unzureichend gesicherte Home-Office-Zugänge und Kollaborationswerkzeuge zu identifizieren und auszunutzen. Die Anzahl der von der Kommunalverwaltung gemeldeten herausgehobene IT-Sicherheitsvorfälle belief sich im letzten halben Jahr monatlich im einstelligen Bereich. Das N-CERT betreut derzeit 104 Kommunen, von denen sich bisher regelmäßig 10% an den Meldungen zum Lagebild beteiligen.

Die Bedrohungslage für die Landes-und Kommunalverwaltung bleibt also unverändert auf erhöhtem Niveau. Zum aktuellen Zeitpunkt werden Angriffe erkannt und geblockt. Es ist davon auszugehen, dass Angreifer ihre Vorgehensweise zukünftig ändern werden, um verbreitete Schutzmaßnahmen zu umgehen.

Zu 1: Herausgehobene IT-Sicherheitsvorfälle wurden bei der Stadtverwaltung Braunschweig bis dato nicht registriert. Jedoch registrieren die städtischen Sicherheitssysteme eine Vielzahl von täglichen Angriffsversuchen. Im Jahr 2016 konnten wir drei lokal begrenzte und zum Teil erfolgreiche Verschlüsselungsangriffe beobachten. Aufgrund dieser Ereignisse und weiterer Entwicklungen von Cyberbedrohungen hat die Stadtverwaltung immer wieder die Einstellungen der eigenen Sicherheitslösungen durch weitere Richtlinien nachgeschärft.

Zu 2: Die Mitarbeitersensibilisierung findet in der Stadtverwaltung fortlaufend und anlassbezogen statt. Sowohl im städtischen Intranet als auch in der Mitarbeiterzeitung WIR erschei-

nen regelmäßig aktuelle Artikel und Hinweise rund um die Informationssicherheit. Anlassbezogen werden auf Informationsveranstaltungen zielgerichtet bestimmte Mitarbeitergruppen geschult. Die Rückmeldungen und Fragen von Mitarbeitern zeigen, dass z.B. schädliche E-Mails sehr wohl als Gefahr wahrgenommen werden. Zudem erfahren Cybersicherheitsmaßnahmen eine hohe Akzeptanz in der Mitarbeiterschaft, obwohl diese den Arbeitsablauf zum Teil behindern. Zu aktuellen Bedrohungen sensibilisiert der IT-Sicherheitsbeauftragte kurzfristig per E-Mail alle städtischen Verwaltungsnutzer bzw. zielgerichtet bestimmbare Organisationseinheiten (z.B. Fachbereich Schule oder Gesundheitsamt).

Zu 3: Die Stadtverwaltung betreibt Schutzsysteme gegen Schadsoftware auf allen IT-System-Ebenen. Bisher haben die umgesetzten Sicherheitsmaßnahmen und die im Einsatz befindlichen Sicherheitssysteme Cyber-Angriffe abwehren können. Die Stadtverwaltung fühlt sich gut aufgestellt und ist sich gleichzeitig bewusst, dass sie im Wettlauf mit der kontinuierlichen Professionalisierung der Angreifer die eigenen Gegenmaßnahmen permanent weiterentwickeln muss ohne eine komplette Sicherheit jemals erreichen zu können. Ein großer Schritt soll durch einen zweiten lokalen Standort für Server im geplanten Business Center III verwirklicht werden. Hier liegt der Mehrwert für die IT-Sicherheit insbesondere auf einer höheren Verfügbarkeit und Ausfallsicherheit der städtischen IT-Systeme. Im Rahmen der Vorplanungen für die Sanierung des Rathaus-Neubaus wird auch eine Versorgung mit Ersatzstrom für einen Notbetrieb im Fall eines Blackouts für den Standort Rathaus untersucht.

Seit Beginn der SARS-CoV-2-Pandemie war in vielen Organisationen eine verstärkte Nutzung von Homeoffice-Zugängen erforderlich. Einige Organisationen haben auf schnelle und in Bezug auf IT-Sicherheit suboptimale Lösungen gesetzt bzw. haben ihre Sicherheitsrichtlinien heruntergesetzt. Die Stadtverwaltung Braunschweig hat seit März 2020 ebenfalls Homeoffice-Zugänge in hoher Anzahl unter Aufrechterhaltung der geltenden Sicherheitsrichtlinien realisiert. Erfahrungen aus dem langjährigen IT-Betrieb für Telearbeit konnten dafür genutzt werden. Aufgrund von neuen Datenschutzanforderungen aus dem Sommer 2020 wurden weitere technische Maßnahmen bezüglich der Sicherheit für Homeoffice-Zugänge bereits umgesetzt. Somit ging und geht das Ermöglichen des Arbeiten im Homeoffice nicht zu Lasten der IT-Sicherheit.

Dr. Kornblum

Anlage/n:

Rückmeldungen der Gesellschaften zur Anfrage 20-14935 „IT-Sicherheit“