Blaustein

Stadt Blaustein
Alb-Donau-Kreis
Beratungsvorlage

Beratungsgremium:	**Gemeinderat**
Sitzung am	**5.11.2019**
Vorlagen Nr.	109 **/2019** ☒ öffentlich ☐ nicht-öffentlich
Amt:	**Haupt- und Personalamt**

Beratungsgegenstand:

Firewallkonzeption mit VPN Anbindung der stadteigenen Liegenschaften und Telearbeitsplätze

Beschlussantrag:

Beschaffung, Umsetzung und Fremdbetrieb einer zweistufigen Firewalllösung für eine Laufzeit von vorerst 5 Jahren. Damit zusammenhängend, die Schaffung von mehreren Netzwerksekmenten zur Erhöhung der Datensicherheit und Anbindung der genannten Liegenschaften.

Thomas Kayser
Bürgermeister

I. Bisherige Beratungs- und Beschlusslage

Gremium	Datum	ö/ nö	Beschluss	Zustimmung/ Ablehnung (einstimmig/ mehrheitlich)
GR	17.07.2018	nö	Vorstellung der Ergebnisse der Analyse zur IT-Infrastruktur der Stadt Blaustein	Kenntnisnahme
GR	11.09.2018	nö	IT-Betrieb optimieren und Betreibermodell ausarbeiten, Kernprozesse optimieren, Ausschreibung einer IT-Stelle	Zustimmung
GR	30.07.2019	ö	Beschaffung von neuer Hard- und Software für die Stadtverwaltung Blaustein	Zustimmung

II. Sachvortrag

Zunächst wird darauf hingewiesen, dass diese Konzeption die Kindergärten, Schulen, Ortsverwaltungen, Gebäude mit Gebäudeleittechnik, das Bad Blau, den Bauhof und die Feuerwehren berücksichtigt.

Ausgangslage:

Rathaus:
Die Stadt Blaustein unterhält aktuell zwei VPN Standleitungen zum Landesverwaltungsnetz, eine Hauptleitung (Erstweg) und eine Backupleitung. Die Voraussetzung hierfür sind zwei Internetverbindungen über die Provider Unitymedia (im Bad-Blau) und die Telekom.
Eine eigene Firewall ist nicht vorhanden, alle Verbindungen nach intern (LVN/KVN) und extern (Internet) werden über diese VPN - Leitungen realisiert. Die Absicherung erfolgt im Rechenzentrum durch eine mehrstufige Firewall.
Für die Telefonie ist ein Multiplexer Telefonanschluss geschaltet, welcher 30 gleichzeitige Telefongespräche zulässt. Diese werden mit einer lokalen veralteten Telefonanlage geführt.

Telearbeit:
Die Möglichkeit für Telearbeit ist momentan für ein sehr begrenztes Benutzerumfeld (16 Benutzer in der Stadtverwaltung und den Schulen) ebenfalls mit dem Rechenzentrum realisiert. E-Mails auf Smartphones können aktuell 10 – 15 Personen der Stadtverwaltung erhalten.

Außenstellen / Liegenschaften:
Für den Bauhof, die Feuerwehr (Hauptwache), die Ortsverwaltungen sowie die Verwaltung des Schulverbundes werden aktuell VPN Festverbindungen durch das Rechenzentrum betrieben. Diese sind aus Kostengründen in der Bandbreite stark begrenzt. Im Schulverbund und der Feuerwehr erfolgt die Datenhaltung aktuell noch dezentral.

In allen anderen Verwaltungseinrichtungen wie Schulen, Ortsfeuerwehren und Kindergärten erfolgt die Datenhaltung jeweils am Standort. Die Daten sind komplett unverschlüsselt und werden individuell gesichert. Die Standorte sind an das Internet angebunden, eine Absicherung durch eine Firewall erfolgt nicht. Die Endgeräte in den Verwaltungseinrichtungen werden auch bezüglich Sicherheit und Software aktuell nicht zentral gesteuert und aktualisiert. Eine gesicherte und verschlüsselte E-Mail Übertragung ist nur an einzelnen Arbeitsplätzen sehr unkomfortabel möglich.
In den Außenstellen / Liegenschaften wird die Telefonie bereits über das Internet realisiert, es findet eine Umsetzung auf die lokalen veralteten Telefonanlagen statt. Diese Umsetzung ist fehlerbehaftet.

Bad Blau:
Das Bad Blau verfügt aktuell über eine Glasfaseranbindung an das Rathaus und eine Internetanbindung über Unitymedia. Die Verwaltungsarbeitsplätze sowie die Kassensysteme und die Technik der Kasseneinrichtung werden logisch gesehen im selben Netz versorgt wie die Rathaus-Arbeitsplätze. Hier findet aktuell keine Trennung statt.
Die Gebäudeleittechnik ist teilweise in einem separaten Netz geführt. Der Netzübergang wird mit einer speziellen Lösung (Bastellösung) realisiert, welche nur sehr instabil funktioniert.
Das öffentliche WLAN von Stadt und Bad-Blau, sowie die EC Bezahlgeräte werden direkt über die Internetleitung abgewickelt.
Die Telefonie läuft über die Telefonanlage im Rathaus.

Gebäudeleittechnik:
Bei der Gebäudeleittechnik wird je Liegenschaft die vorhandene Internetleitung verwendet. Eine separate Absicherung durch eine Firewall findet nicht statt. Die Steuerung erfolgt durch Notebookgeräte, die ebenfalls über einen direkten und ungesicherten Internetzugang verfügen.

Soll-Konzeption:

Internetanbindung Rathaus und Liegenschaften:
Die Telefon- und Internetverträge aller Liegenschaften sowie die möglichen Bandbreiten werden auf Verbesserungen und Konsolidierung geprüft. Entsprechende „Flottenverträge" mit den Anbietern werden angestrebt. Anfragen hierfür sind bei den Anbietern: SWU, Telekom und Unitymedia gestellt. Eine Umstellung soll im Jahr 2020 sukzessive erfolgen, um für alle Standorte die wirtschaftlichste Anbindung zu erhalten.

Im Rathaus soll ein zweistufiges Firewall Konzept realisiert werden. Damit werden zwei Firewall Systeme verschiedener Hersteller in Reihe geschaltet. Dies ist nötig, um die Anforderungen des Bundesamtes für Sicherheit (BSI) vollumfänglich zu erfüllen.
Folgende Funktionen muss die Firewall bzw. die zwei Firewall Systeme erfüllen, um in Zukunft alle Anforderungen der Stadt Blaustein erfüllen zu können:

- Komplettes Management durch den Lösungsanbieter in Verbindung eines Servicevertrages
- Breitbandanbindung über mindestens zwei Provider (Telekom / Unitymedia) an das Internet. Dies erfolgt aus Gründen der Geschwindigkeit und Ausfallsicherheit

- Anbindung aller Liegenschaften über VPN direkt vom Rathaus aus mit deutlich mehr Bandbreite als bisher (ca. 20)
- Eigene Sicherheitsbereiche (logische Netze) für die Bereiche Telearbeitsplätze, Arbeitsplätze Rathaus, Arbeitsplätze Feuerwehren, Arbeitsplätze Schulverwaltungen, Arbeitsplätze Bad Blau, Arbeitsplätze Kindergärten, Gebäudeleittechnik Liegenschaften, Zeiterfassung, Telefonie, Gebäudeleittechnik Bad Blau und Kassenumgebung Bad Blau
- Prox und Reverse-Proxy Funktionalität mit Paketfilter
- Eine großzügige Anzahl (>= 50) der möglichen Telearbeitsplätze muss ohne Mehrkosten möglich sein
- Eine großzügige Anzahl (>= 50) der mobilen Office Anbindungen (Mail, Kalender, etc. auf das Handy) muss möglich sein
- Eine Zertifizierungsstelle und einen Radiusserver, um eine Zweifaktorauthentifizierung zu realisieren
- Vorbereitung für Vereinheitlichung und Umstellung der Telefonie 2020
- Eine eigene DMZ für extern wirksame Systeme wie z.B. ein Managementserver für mobile Geräte oder EC Bezahlsysteme

Telearbeit:

Die Möglichkeit für Telearbeit soll nach Bedarf für mindestens 50 Mitarbeiter auf nahezu jedem Computer (z.B. PC zu Hause) möglich sein. Erforderlich ist eine Zweifaktorauthentifizierung, mit einem Kennwort und z.B. einem zufällig generierten Code per SMS. Auch die Telefonie für Telearbeiter soll über diesen Weg zukünftig möglich sein.

Außenstellen / Liegenschaften:

Alle Außenstellen / Liegenschaften werden per VPN angebunden. Je nach Anforderung werden auf die Anbindung die jeweilig benötigten Netze / Sicherheitsbereiche aufgeschaltet. Die Geschwindigkeit richtet sich nach dem Provider und der tatsächlich benötigten Bandbreite. Alle dezentral gelagerten Daten werden in das Rathaus übertragen und dort zentral gesichert. Eine Bearbeitung der Daten erfolgt ab diesem Zeitpunkt ausschließlich auf den zentralen Servern im Rathaus. Auch eine gesicherte Anbindung der E-Mailanbindung an das LVN / KVN wird über diese Anbindung realisiert. Die Voraussetzungen wurden bereits mit der Serverbeschaffung dieses Jahr geschaffen. Die Kommunikation der Zeiterfassungsgeräte wird ebenfalls über diese Anbindung sichergestellt. Alle Voraussetzungen für eine VOIP Telefonie 2020 werden hergestellt.

Bad-Blau:

Strikte Trennung der Kassensysteme von den Verwaltungsarbeitsplätzen und der Gebäudeleittechnik. Die Trennung ist notwendig, um den jeweiligen Servicepartnern auf die zu unterstützenden Systeme Zugriff zu gewähren. Alle Voraussetzungen für eine VOIP Telefonie 2020 werden hergestellt. Abwicklung des öffentliche WLAN sowie die EC Bezahlgeräte in der DMZ (Demilitarisierte Zone, die DMZ ist ein eigenständiges Subnetz, dass das lokale Netzwerk durch Firewall-Router vom Internet trennt).

Gebäudeleittechnik:
Bereitstellung eines separaten Netzes für die Gebäudeleittechnik in Vorbereitung für ein Herstellerübergreifendes System, welches die Steuerung aller Liegenschaften zulässt. Zusätzliche Absicherung der Gebäude Leittechnik zum Internet, mit Bereitstellung von Fernwirkmöglichkeiten für externe Servicepartner.

Fazit:

Zukünftig werden Kosten gespart, durch die Firewall-Konzeption mit der VPN-Anbindung wird deutlich mehr Funktionalität und Sicherheit geboten. Herr Pfeiffer wird das Konzept in der Sitzung vorstellen und steht für Fragen zur Verfügung.

Die Verwaltung beantragt, die Zustimmung zur Firewallkonzeption mit VPN-Anbindung.

III. Finanzierung

Derzeit läuft noch die Angebotseinholung. Die bisher geschätzten Kosten werden sich auf ca. 60.000€ belaufen. Sobald die Angebote vorliegen werden die Kostenkalkulation sowie die Berechnung der laufenden Kosten sowie die Einsparungen noch vor der Sitzung nachgereicht.

Haushaltsstelle	**HH-Ansatz (Euro)**	**Noch verfügbare Mittel (Euro)**	**Geplante Ausgaben (Euro)**	**Überplan-mäßig/ außerplan-mäßig**
M 06300001 9350 /9410	140.000€	0€ (bei Beschluss-fassung zu AIDA)	Ca. 60.000€	Ca. 60.000€ Überpl.

Anmerkungen zur Finanzierung:

Der Kindergarten Herrlingen kann nicht mehr in diesem Haushaltsjahr wie geplant abgewickelt werden, daher ist eine Deckung mit Blick auf den Gesamthaushalt möglich. Bei der Haushaltsstelle M 06300001 9350/9410 ist daher nach Rücksprache mit dem Kämmerer eine überplanmäßige Ausgabe möglich.

26.10.2019

Benjamin Pfeiffer
IT-Beauftragter

Anke Jaeger
Haupt- und Personalamtsleitung