Der Oberbürgermeister

Amt: Hauptamt

AZ: 10 10 57

Informationsvorlage- Nr. IV 0043/20 öffentlich

Betreff: Aktueller Stand zur IT-Sicherheit der Stadt Bernburg (Saale)

Kenntnisnahme	18.06.2020	Abstimmungsergebnis:			Änderung des
		Ja	Nein	Enth.	Beschlussvorschlages
Stadtrat		☐	☐	☐	☐

Finanzielle Auswirkungen

Nein

Auszüge vorbehaltlich der Genehmigung sind zuzuleiten:

Amt: I/10 Hauptamt/EDV

(ansonsten Protokolle im Intranet)

Aufgestellt:
Herr Tschöpe

Amt:
I/10

mitgezeichnet:
Herr Hohl - Hauptamtsleiter
Frau Dr. Ristow - Dezernentin I

- Oberbürgermeister -

Inhaltsbeschreibung:

In dieser Informationsvorlage soll dargestellt werden, welche Maßnahmen die Stadt Bernburg (Saale) seit Ende 2017 durchgeführt hat und weiter durchführen wird, um die Sicherheit der IT-Infrastruktur der Stadt zu gewährleisten und zukünftig qualitativ zu verbessern.

Sachverhalt:

1. Einleitung

Die IT-Infrastruktur der Stadt Bernburg (Saale) wird durch die EDV-Abteilung des Hauptamtes der Stadt Bernburg (Saale) aufgebaut, erweitert und verwaltet. Aktuell sind vier Mitarbeiter mit der Verwaltung der Infrastruktur betraut. Aufgrund eines Sicherheitsvorfalles innerhalb der IT-Infrastruktur im Oktober 2017 wurde das Sicherheitskonzept überarbeitet und erweitert.

In dieser Informationsvorlage soll dargestellt werden, welche Maßnahmen seit Ende 2017 durchgeführt wurden und weiter durchführen werden, um die Sicherheit der IT-Infrastruktur der Stadt Bernburg (Saale) zu gewährleisten und zukünftig qualitativ zu verbessern.

2. Übersicht der technischen Infrastruktur der Stadt Bernburg (Saale)

Die IT-Infrastruktur der Stadt Bernburg (Saale) umfasst die Kernverwaltung in vier Rathäusern, die Feuerwehr samt Ortsfeuerwehren, den Betriebshof mit Stadtarchiv und Friedhof, 14 Kindertageseinrichtungen, fünf Grundschulen, das Klubhaus der Jugend, die Jugendherberge sowie das Sozialzentrum.

Das zentrale Rechenzentrum der IT-Infrastruktur befindet sich im Rathaus I. Die Rathäuser II – IV sind jeweils über Glasfaser an das zentrale Rechenzentrum angeschlossen. Die Feuerwehr in Bernburg (Saale) und der Betriebshof mit Stadtarchiv sind jeweils über eine verschlüsselte VPN-Verbindung¹ an das Rechenzentrum angebunden. Die weiteren nachgeordneten Einrichtungen sind aktuell nicht direkt mit dem Rechenzentrum verbunden.

3. Neuerung in der IT-Sicherheit seit 2017

Seit dem Sicherheitsvorfall im Oktober 2017 wurde das Sicherheitskonzept der Stadt Bernburg (Saale) grundlegend überarbeitet, Schwachstellen analysiert und ausgebessert sowie die IT-Infrastruktur so aufgestellt, dass sie auch künftig gegen technische Angriffe und Schadsoftware abgesichert ist.

Folgende Einzelmaßnahmen wurden seitdem durchgeführt:

1. Für die Standorte des zentralen Rechenzentrums, der Feuerwehr in Bernburg (Saale) und des Betriebshofs mit Stadtarchiv wurde jeweils eine **neue Hardware-Firewall**

¹ VPN= virtuelles privates Netzwerk – geschlossenes und verschlüsseltes Kommunikationsnetz zur Anbindung verschiedener Datennetze

eingrichtet. Diese analysiert den ein- und ausgehenden Netzwerkverkehr auf Schadsoftware und Bedrohungen und blockiert diesen. Darüber hinaus können durch verschiedene Filterregeln unerlaubte Downloads blockiert, der Aufruf schadhafter Internetseiten unterbunden und externe technische Angriffe geblockt werden.

Über eine verschlüsselte Verbindung erlaubt sie die sichere Anbindung der Standorte Feuerwehr und Betriebshof an das zentrale Rechenzentrum zur gemeinsamen Nutzung von Daten und Programmen.

2. Der **Spamfilter** des zentralen Mailserver wurde **erweitert und verschärft**. Dieser blockiert nun E-Mails mit weiteren Schlagwörtern und Eigenschaften, die darauf schließen lassen, dass es sich dabei um schadhafte E-Mails handeln könnte.

Darüber hinaus werden Office-Dokumente (Word-, Excel- und PowerPoint Dateien) mit integrierten Makros (ausführbaren Inhalten) geblockt, da aufgrund dieser ausführbaren Inhalte unerwünschte und schadhafte Dateien im Hintergrund heruntergeladen werden können (bekannte Emotet Schadsoftware).

3. Zusätzlich zu Punkt 2 wurde durch Richtlinien eingestellt, dass **Makros in Office-Dokumenten grundsätzlich nicht ausführbar** sind, um das Herunterladen von unerwünschten und schadhaften Dateien im Hintergrund zu unterbinden. Dies ist notwendig, um auch Office-Dokumente, die nicht per E-Mail in die IT-Infrastruktur gelangen oder die vom Spamfilter nicht erkannt werden, zu blockieren.
4. Die **Berechtigungen der Verwaltungsmitarbeiter** am Arbeitsplatz-PC wurden so **eingeschränkt**, dass auch ausnahmsweise keine administrativen Rechte vergeben werden und die Mitarbeiter nicht in der Lage sind, eigenständig Software zu installieren. Dies ist notwendig, damit sich Schadsoftware nicht die etwaigen administrativen Rechte des Mitarbeiters abgreifen kann und selbstständig weitere Schadsoftware herunterladen und installieren kann.

Das Arbeitskonto des Mitarbeiters und sein administratives Konto (ohne Zugriff durch den Mitarbeiter) sind strikt voneinander getrennt.

5. In der Kernverwaltung der Stadt Bernburg (Saale) (Rathäuser I – IV) wurde ein **neues Antivirensystem** eingeführt. Dieses nutzt nicht mehr, wie bisherige Antivirensysteme, Muster von Schadsoftware um diese zu erkennen und zu blockieren, sondern blockiert gezielt die Angriffswege, die eine Schadsoftware nutzen würde, um ein System zu befallen.

Dies hat den Vorteil, dass der Antivirenhersteller nicht mehr regelmäßig die Muster anhand neuer Schadsoftware aktualisieren muss (zurzeit mehr als 350.000 neue Schadsoftware pro Tag²), sondern gezielt einige wenige Angriffswege schützen muss, die die Schadsoftware ausnutzen kann. Ein weiterer Vorteil ist, dass Schadsoftware, die von bisherigen Systemen nicht als solche erkannt wurde, dennoch blockiert werden kann, da die auszunutzenden Angriffswege überwacht und blockiert werden (z. B. Verschlüsselungstrojaner).

² <https://www.av-test.org/de/statistiken/malware/>

6. Die **Verwaltungsmitarbeiter** wurden **geschult und sensibilisiert**, um digitale Inhalte vorsichtig und aufmerksam zu bewerten. Gerade beim Thema E-Mail wurde den Mitarbeitern mehrfach gezeigt, dass ein achtsamer Umgang mit E-Mails und deren Anhängen oftmals bereits das Einfangen von Schadsoftware verhindern kann. So sollen die Mitarbeiter genauer darauf achten, dass die E-Mail von einem vertrauenswürdigen Absender stammt, keine unbekanntes und gekürzten Links anzuklicken und Anhänge nicht ungeprüft zu öffnen sind.
7. Die Möglichkeit **externe Datenträger** an Arbeitsplatz-PC anzuschließen wurde grundsätzlich **blockiert**, um schadhafte Datenträger von externen Personen nicht ungeprüft durch den Mitarbeiter anzuschließen und Schadsoftware auf den PC zu laden. Das Ziel ist es, Daten mithilfe von zeitgemäßen und sicheren Übertragungswegen (verschlüsselte E-Mails und datenschutzkonforme Cloudlösungen) auszutauschen.
8. Bei der Einrichtung neuer Arbeitsplatz-PC wird der **BIOS-Zugang³ mit einem Passwort geschützt**. Dies soll verhindern, dass jemand mit physischem Zugang zum Gerät Zugriff auf das BIOS erhält, ein externes System startet und Daten entwenden kann.
9. In mehreren Verwaltungsbereichen wurde die **Übertragung von personenbezogenen Daten** per E-Mail auf einen **verschlüsselten Versand⁴** umgestellt. Damit sollen zum einen die datenschutzrechtlichen Anforderungen der DSGVO eingehalten und zum anderen der sicherheitstechnische Schutz von sensiblen Daten gewährleistet werden.
10. Es wurde begonnen, die **Netzwerkinfrastruktur** in den Rathäusern so zu **trennen**, dass verschiedene Dienste (z.B. Datenverkehr und Telefonie) verschiedene Netzwerksegmente nutzen. Dadurch soll verhindert werden, dass bei einem Schadsoftwarebefall einer Netzwerkkomponente nicht sofort das gesamte Netzwerk befallen, sondern an entsprechenden Schnittstellen aufgehalten wird und die befallenen Teilnetzwerke zur Bereinigung abgeschaltet werden können.
11. Innerhalb der IT-Infrastruktur wurde eine **zentrale Zertifikatsinfrastruktur aufgebaut** (Public-Key-Infrastruktur PKI). Solch eine Zertifikatsinfrastruktur stellt digitale Zertifikate aus, verteilt diese innerhalb des Datennetzes und überprüft sie auf ihre Gültigkeit. Ein digitales Zertifikat dient der Absicherung der elektronischen Kommunikation innerhalb der IT-Infrastruktur indem es die Vertrauenswürdigkeit eines Absenders bestätigt. Zusätzlich dazu wird die entsprechende Kommunikation auf ihrem Transportweg verschlüsselt. So kann gewährleistet werden, dass die digitale Kommunikation nicht von einem unberechtigten Dritten abgefangen und manipuliert wird.

Dies wird beispielsweise bei der Kommunikation zwischen Antivirensystem auf dem Arbeitsplatz-PC und dem Antiviren-Server angewendet.

4. Finanzielle Aufwendungen für die IT-Sicherheit seit 2017

³ BIOS= Basic Input/Output System – Steuereinheit des Computers, welche das eigentliche Betriebssystem Windows startet

⁴ Ende zu Ende Verschlüsselung, d. h. die E-Mail wird vom Absender verschlüsselt und erst vom Empfänger wieder entschlüsselt

Folgende finanzielle Aufwendungen wurden getätigt, um die Punkte aus 3. gemeinsam mit externen Dienstleistern zu realisieren:

Nr.	Maßnahme	Kosten brutto
	Grundlage: Erneuerung der Hardware im zentralen Rechenzentrum	239.000 €
3.1	neue Firewall Rathäuser inkl. Herstellersupport für 5 Jahre	62.000 €
3.1	neue Firewall Feuerwehr Bernburg (Saale) inkl. Herstellersupport für 5 Jahre	5.000 €
3.1	neue Firewall Betriebshof inkl. Herstellersupport für 5 Jahre	5.000 €
3.5	neues Antivirensystem inkl. Herstellersupport für 5 Jahre	23.000 €
3.1 + 3.5	monatliche Auswertung der Firewall und des Antivirensystems auf Bedrohungen und Angriffe mit externem Expertenteam	2.700 € monatlich
3.11	Aufbau einer Zertifikatsinfrastruktur	6.000 €

Alle weiteren Maßnahmen aus 3. wurden ausschließlich durch die Mitarbeiter der EDV-Abteilung durchgeführt.

5. Mittelfristige Pläne für die IT-Sicherheit

Aufgrund der Entwicklung immer neuer Schadsoftware ist die Stadt Bernburg (Saale) gezwungen, stets neue Maßnahmen zu treffen, um die Absicherung der IT-Infrastruktur zu gewährleisten. Somit ist IT-Sicherheit ein Thema, welches nie komplett abgeschlossen sein wird, sondern einer stetigen Weiterentwicklung bedarf.

Mittelfristig sind folgende Maßnahmen zur Absicherung der IT-Infrastruktur geplant:

1. **Einrichtung eines neuen Mailfilters**, um die Filterung von schadhafte E-Mails und E-Mails mit schadhafte Anhängen noch gezielter und zuverlässiger steuern zu können
2. schrittweise Abkehr von der Filterung von Spam-Mails hin zum **Blockieren und Zurücksenden von Spam-Mails** an den Absender

3. Aufbau eines **neuen E-Mail-Servers** zur kompletten Reorganisation des E-Mail-Systems und der weiteren Unabhängigkeit von externen Dienstleistern und auch zur Reduzierung etwaiger Ausfallzeiten des E-Mail-Systems
4. schrittweiser Ausbau der **verschlüsselten E-Mail-Kommunikation** in weiteren Verwaltungsbereichen
5. weitere **Trennung der Netzwerkinfrastruktur** vor allem zwischen Arbeitsplatz-PC und Server-Systemen, um bei einem Befall von Arbeitsplatz-PC den Befall der Server-Systeme zu verhindern
6. weitere **Anbindung von nachgeordneten Einrichtungen** an das zentrale Rechenzentrum mit einer verschlüsselten VPN-Verbindung (Friedhof, Sozialzentrum, Jugendherberge, Ortsfeuerwehren)
7. Im Zuge der Schul-IT werden die **Grundschulen** der Stadt Bernburg (Saale) mit einer **zeitgemäßen IT-Infrastruktur und flexiblen Endgeräten** für Lehrer und Schüler ausgestattet. Auch diese IT-Infrastrukturen sollen über verschlüsselte VPN-Verbindungen **an das zentrale Rechenzentrum angebunden** werden.
8. stetige **Anpassungen der Regeln** der Firewall und des Antivirensystems, um auch zukünftige Schadsoftware zuverlässig zu erkennen und zu blockieren
9. Alle **Mitarbeiter** werden ständig **fortgebildet**, um ein umfangreiches Grundverständnis zu Sicherheitsbedrohungen zu entwickeln und Sicherheitsvorfälle durch Fehleinschätzungen und Fehlbedienungen zu vermeiden.
10. Als Grundlage zur IT-Sicherheit wird die eingesetzte Hard- und Software ständig den aktuell erforderlichen technischen Gegebenheiten angepasst. Durch sich ständig weiterentwickelnde Sicherheitsbedrohungen sind **Aktualisierungen von Hard- und Software** notwendig, um Sicherheitslücken zu schließen und zeitgemäße Sicherheitsverfahren nutzen zu können, wodurch kontinuierlich Kosten und ein höherer Personalbedarf entstehen.