

KREISSTADT METTMANN Die Bürgermeisterin		Drucksachennummer 409.5/2021	
Beschlussvorlage			
Abteilung für IT-Service	öffentlich	☒	
Tran, Van Kiem	nicht öffentlich	☐	

Gremium:	TOP-NR:	Datum:
Haupt- und Finanzausschuss	8	30.11.2021

Mittelfreigaben
 Erneuerung der Firewall

<u>Finanzielle Auswirkungen</u>	nein
Kosten	200.000 €
Produkt	01.01.08 E-Government und IT-Service
Haushaltsjahr	2021
Folgekosten	
Haushaltsmittel stehen zur Verfügung	☒ ja ☐ nein
Deckungsvorschlag	

Anmerkung der Stadtkämmerin:

UMWELTBELANGE werden besonders berührt im Bereich:

☐ Abfall	☐ Wasserhaushalt	☐ Klima
☐ Boden	☐ Natur- und Artenschutz	☐ Emissionen / Immissionen

BESCHLUSSVORSCHLAG
 Die Mittel für die Erneuerung der Firewall werden in Höhe von 200.000 Euro für 2021 freigegeben.

Abstimmungsergebnis:

	Ja	Nein	Enthaltungen
CDU			
Die Grünen			
SPD			
FDP			
Zur Sache!ME			
WGME			
AfD			
Die Linke			
Bürgermeisterin			

Verwaltungserläuterung:**Firewall:**

Im Jahr 2013 hat die Verwaltung die seinerzeit abgekündigte Cisco PIX-Firewall durch ein redundantes Cisco Firewall ASA-5545-X-System ersetzt. **Die Firewall schützt technisch – soweit möglich - das gesamte interne Netz und die Systeme der Kreisstadt Mettmann vor unberechtigten Zugriffen.** Die Kreisverwaltung bzw. das Kommunales Rechenzentrum Niederrhein (KRZN) ist der Internet Provider der Kreisstadt Mettmann und bindet diese per Glasfaserleitung an. Die Firewall bildet die Schnittstelle zum städtischen Netz und schützt dieses vor externen Bedrohungen wie beispielsweise unberechtigten Zugriffen oder auch DOS Attacken. Die Firewall der Kreisverwaltung (bzw. des KRZN) ist für die Kreisstadt Mettmann transparent. Die städtische Firewall schützt das Netz der Kreisverwaltung nicht, dafür ist die Firewall der Kreisverwaltung zuständig und umgekehrt.

Betrieben wird das Netz der Kreisstadt Mettmann sowie die Firewall intern in der Verwaltung durch die Abteilung IT.

Die lokalen Außenstellen (wie beispielsweise der Baubetriebshof, die Erziehungsberatungsstelle, die Bibliothek oder städtische Kindertageseinrichtungen) sind per Ethernet Connect Standleitung der Telekom angebunden. Die Home-Office-Arbeitsplätze sind mit dem Netz der Stadtverwaltung über VPN verbunden.

Die Firewall verfügt über Syslog Message, in dem Aktivitäten und Vorkommnisse (Monitoring) festgehalten werden. Die jetzige Cisco Firewall ist eine „traditionelle Firewall“, die auf der Grundlage von Status, Port und Protokoll entscheidet, ob Datenverkehr zugelassen oder blockiert wird. Die Filterentscheidungen werden durch festgelegte Regeln getroffen.

Die Cisco ASA 5545-X-Reihe wird seit Sept. 2020 nicht mehr neu von CISCO verkauft, ein Support wird noch bis 30.Sept. 2025 angeboten.

Die neue Cisco Firepower Next-Generation Firewall der Reihe 4125 soll die alte Cisco ASA 5545-X-Firewall ablösen. Die Cisco Firepower 4125 ist eine integrierte, bedrohungsorientierte Next-Generation Firewall, die unter anderem über folgende Funktionen verfügt:

- Next-Generation Intrusion Prevention System (NGIPS) für Schutz vor Bedrohung,
- vollständig integrierte Advanced **Malware Protection** – Lösung (AMP), die wirksamen Schutz gegen bekannte und unbekannte Bedrohungen bietet,
- Funktion zur **Verfolgung und Eindämmung von Malware-Infektionen**,
- automatische Korrelation von Bedrohungsereignissen mit Schwachstellen im Netzwerk, damit die Ressourcen zur Abwehr der wichtigsten Bedrohungen verfügbar sind,
- Analyse von Schwachstellen im Netzwerk.

Mit diesen zusätzlichen Eigenschaften wird das Stadtnetz künftig auch gegen moderne Angriffsvektoren stärker geschützt sein. Selbstverständlich gewährleisten diese automatischen Systeme einen Rundumschutz. Ein erfolgreiches Angriffsszenario wird damit unwahrscheinlicher. Bei der Cisco Firepower 4125 handelt es sich wie bereits dargelegt um eine sogenannte Next Generation Firewall. Diese wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für einen effektiven Schutz von Bedrohungen, die durch komplexe und schwere Malware-Angriffe entstehen, empfohlen.

Insgesamt lässt sich festhalten, dass durch die Einführung der Cisco Next-Generation Firewall die IT-Sicherheit der Netzinfrastruktur der Verwaltung gegen verschiedene Gefährdungslagen und spezifische Bedrohungen erhöht wird.

Angesichts des fortgeschrittenen technischen Alters der Firewall sowie der stetig zunehmenden Gefahren aus dem Internet ist es dringend notwendig, die vorhandene städtische Firewall als eine Maßnahme im Rahmen eines ganzheitlichen Sicherheitskonzeptes zu erneuern.

Im Hinblick auf die lange Lieferzeit der Cisco-Systeme von aktuell 6 Monaten und länger, möchte die Verwaltung mit der Umsetzung beginnen und die Bestellung auf den Weg bringen.

Die neue Firewall wird über den Rahmenvertrag mit dem KRZN beschafft, so dass es keiner gesonderten Ausschreibung bedarf und mithin eine kurzfristige Beauftragung möglich ist.

Darüber hinaus nimmt die Installation und Inbetriebnahme zusätzliche Zeit in Anspruch. Die neue Firewall muss parallel zur bestehenden Firewall aufgebaut, eingerichtet und getestet werden.

Somit ist für die finale Umstellung auf die neue Firewall mit einem Zeitaufwand von bis zu einem Jahr zu rechnen

Es wird dringend empfohlen den Austausch der alten Firewall vor Erreichen der 10 Jahres-Grenze zu realisieren.

Die Verwaltung hat daher für die Erneuerung der Firewall entsprechende Mittel in den Haushalt eingestellt. Um die Freigabe der Mittel in Höhe von 200.000 € wird gebeten.

Gez. Kotthaus

gez. Pietschmann