Stadt Köln

Die Oberbürgermeisterin

Dezernat, Dienststelle
I/12

Vorlagen-Nummer
3474/2015

Beantwortung einer Anfrage nach § 4 der Geschäftsordnung

öffentlicher Teil

Gremium	Datum
Unterausschuss Digitale Kommunikation und Organisation	22.02.2016

Contentfilter städtisches Internetangebot; Beantwortung der Anfrage AN/1625/2015 der Gruppe Deine Freunde

Die Verwaltung nimmt wie folgt Stellung:

Frage 1: Wer ist der Contentfilterhersteller? Was versteht dieser Hersteller unter "negativer Reputation", anhand welcher Kriterien erhalten einzelne Webseiten dieses Merkmal – oder auch nicht?

Antwort:
Als Internet-Contentfilter wird bei der Stadt Köln das Produkt „WebGateway“ des Herstellers McAfee GmbH (Intel Security) eingesetzt. WebGateway stellt diverse Funktionen zum Schutz der städtischen Infrastruktur, bzw. der Daten im städtischen Netzwerk bereit wie z.B. Anti-Malware-Scanner, Mediatype-Filter, URL- und die Reputations-Filter.
Die URL- und Reputationsfilter basieren u.a. auf „TrustedSource“. Dies ist ein ursprünglich von CipherTrust entwickeltes und mittlerweile von McAfee betriebenes „Leumunds“-System für Webpräsentationen.
TrustedSource erstellt Echtzeit-Profile aller Internet-Präsenzen und -Webseiten, sowie von IP-Adressen auf der Grundlage von Hunderten verschiedenen Attributen, die durch die umfangreichen weltweiten Datenerfassungskapazitäten von McAfee Labs analysiert werden. Anschließend ordnet die Lösung Reputations-Bewertungen (nummerische Werte) zu, die auf dem ermittelten Sicherheitsrisiko beruhen. Diese Bewertungen werden in das Regelwerk des Contentfilters übernommen und filtern mit dieser präventiven Absichtsanalyse in Echtzeit gefährliche Inhalte aus dem Web-Datenverkehr heraus. Durch Scannen des aktiven Inhalts einer Webseite, Emulieren sowie Erfassen seines Verhaltens und Vorhersagen seiner Absicht schützt McAfee Web Gateway präventiv vor Zero-Day- und gezielten Angriffen, sobald diese stattfinden.

Frage 2: Warum erhält die Seite antifa-koeln.net die Wertung negative Reputation, und was bedeutet in diesem Zusammenhang „Medium Risk (30)“?

Antwort:
Die Reputation, der Leumund einer Webseite, wird von McAfee technisch auf einer Skala von -128 bis +128 nach einem hochkomplexen und umfangreichen Prozess bewertet (s.o.). Im Contentfilter-System sind drauf basierende Filterregeln konfiguriert, die sich zum einen auf die Erfahrung der letzten Jahre sowie auch nach Herstellerempfehlung richten. Im Fall von www.antifa-koeln.net wurde ein Reputationswert von 30 Punkten mit einem mittleren Sicherheitsrisiko vom Hersteller bewertet. Es gibt für Kunden keine Möglichkeit die Basis der Bildung des Reputationswertes einzusehen.
Es kann in Ausnahmefällen zu Fehleinschätzungen (False-Positives) durch den Contentfilter-Hersteller kommen. In diesen Fällen kann die Stadt Köln als Kunde auf direktem Weg eine Prüfung und Korrektur beim Hersteller anfordern.
Für www.antifa-koeln.net wurde diese Prüfung durch McAfee am 29.10.15 beauftragt und McAfee hat

das Risiko auf ein Minimum herunterstuft (Fehlindizierung), mit dem nächsten inhaltlichen Datenbankupdate, welches alle 6 Stunden durchgeführt wird, ist die Webseite dann erreichbar.

Frage 3: Werden Ratsmitglieder, sowie weitere politische Mandatsträger und ihre Mitarbeiter als eigene Nutzergruppe des Internet-Angebotes der Stadtverwaltung geführt?

Antwort:
Ja, das ist der Fall.

Frage 4: Falls JA bei Frage 3: Welche Filter wurden für diese Nutzergruppe mit dem Hersteller vereinbart? Hat die Verwaltung Einfluss auf die Auswahl der blockierten Seiten?
Falls NEIN bei Frage 3: Welche weiteren Nutzergruppen unterliegen ähnlichen Beschränkungen? Hält die Verwaltung die Gleichstellung dieser Nutzergruppen für gerechtfertigt?

Antwort:
Für die Benutzergruppe der Mandatsträgerinnen und Mandatsträger ist der „erweiterte Internetzugang“ freigeschaltet, welcher den Zugriff auf nahezu alle Internet-Inhalte ermöglicht.
Sicherheitskritische Internetpräsenzen und -Seiten werden über die URL-Kategorien stadtweit geblockt und sind nicht zugelassen, darunter fallen z.B. Browser Exploits, Malicious Downloads, Malicious Sites, Phishing, Potential Hacking/Computer Crime, Spam URLs, Spyware/Adware/Keyloggers, da sie die Daten im städtischen Netzwerk gefährden.

Ergänzend zu den Kategorien wird ein Zugriff auf eine Webseite bei einem Reputationswert >29 (mittleres Risiko) unterbunden sowie bei einer automatischen Detektion von Schadcode.
In Zusammenarbeit der Fraktionen mit dem IT-Sicherheitsverantwortlichen wurden sog. URL-Kategorien definiert, welche für die Benutzergruppe permanent freigeschaltet sind und diese wurden im Beirat für Sicherheit und Kommunikation mit Informationstechnik (SKIT) abgestimmt.

Frage 5: Wäre es im Sinne der Gewährleistung einer uneingeschränkten Arbeitsmöglichkeit der Mandatsträger nicht sinnvoller sämtliche Beschränkungen aufzuheben?

Antwort:
Aufgrund der potentiellen Gefährdung der gesamten städtischen Infrastruktur, bzw. der Daten und unter Umständen auch der Infrastrukturen angeschlossener Partner wie z.B. andere Behörden durch z.B. Viren ist eine uneingeschränkter Internetzugang ohne Schadecode-Detection, Reputationsfilter und Filterung kritischer Kategorien nicht umsetzbar.
Allerdings können Mandatsträgerinnen und Mandatsträger über mobile Geräte wie z.B. iPad jederzeit uneingeschränkt auf das Internet zugreifen, da sich diese Geräte außerhalb der städtischen Infrastruktur bewegen und somit keine Gefährdung für die städtischen Daten vorliegt.