

BESCHLUSSVORLAGE V0073/16 öffentlich	Referat	Referat OB/ZV
	Amt	Amt für Informations- und Datenverarbeitung
	Kostenstelle (UA)	0210
	Amtsleiter/in	Werner, Johann
	Telefon	3 05-11 00
	Telefax	3 05-11 20
E-Mail	edv@ingolstadt.de	
Datum	27.01.2016	

Gremium	Sitzung am	Beschlussqualität	Abstimmungs- ergebnis
Finanz- und Personalausschuss	18.02.2016	Entscheidung	

Beratungsgegenstand

Projektgenehmigung für die Einführung eines Systems zum detaillierten Management aller Zugriffsberechtigungen im IT-Netzwerk der Stadt Ingolstadt
(Referent: Herr Siebendritt)

Antrag:

Die Projektgenehmigung für die Einführung eines Systems zum detaillierten Management aller Zugriffsberechtigungen im IT-Netzwerk der Stadt Ingolstadt wird erteilt.
Die Gesamtprojektkosten für drei Jahre in Höhe von ca. 140.000 € (brutto) werden genehmigt.

gez.

Christian Siebendritt
Berufsmäßiger Stadtrat

Finanzielle Auswirkungen:

Entstehen Kosten: ja nein

wenn ja,

Einmalige Ausgaben 140.000,--	Mittelverfügbarkeit im laufenden Haushalt	
Jährliche Folgekosten 25.000,-- ab 2019	<input checked="" type="checkbox"/> im VWH bei HSt: 0.021000.611000 <input checked="" type="checkbox"/> im VMH bei HSt: 1.021000.935100	Euro:
Objektbezogene Einnahmen (Art und Höhe)	<input type="checkbox"/> Deckungsvorschlag von HSt: von HSt:	Euro:
Zu erwartende Erträge (Art und Höhe)	von HSt:	
	<input type="checkbox"/> Anmeldung zum Haushalt 20	Euro:
<input type="checkbox"/> Die Aufhebung der Haushaltssperre/n in Höhe von Euro für die Haushaltsstelle/n (mit Bezeichnung) ist erforderlich, da die Mittel ansonsten nicht ausreichen.		
<input type="checkbox"/> Die zur Deckung herangezogenen Haushaltsmittel der Haushaltsstelle (mit Bezeichnung) in Höhe von Euro müssen zum Haushalt 20 wieder angemeldet werden.		
<input type="checkbox"/> Die zur Deckung angegebenen Mittel werden für ihren Zweck nicht mehr benötigt.		

Kurzvortrag:

Mittlerweile berichten die Medien fast täglich über den unerlaubten Zugriff auf teils riesige und sensible Datenbestände von Unternehmen und Behörden. Immer wieder gelingt es immer professioneller arbeitenden Hackergruppen, zielgerichtet große Schäden anzurichten. Kaum war der Hackerangriff auf dem Bundestag im Mai letzten Jahres bekannt geworden, so richteten sich bereits im Juni Attacken auf zahlreiche Zulassungsbehörden in Hessen und Rheinland-Pfalz. Auch das IT-Netzwerk der Stadt Ingolstadt wird regelmäßig angegriffen, die getroffenen Schutzmaßnahmen haben sich bislang aber stets bewährt.

Um einen umfassenden und hochwertigen Schutz der Daten zu erreichen, sind neben der Abwehr von unerlaubten Zugriffen von außen aber auch weitere Maßnahmen im Inneren des Netzes notwendig. Derzeit werden vom Systemmanagement der Stadt Ingolstadt ca. 3.600 Kennungen und 2.700 Postfächer verwaltet (tatsächliche Mitarbeiter/innen und zahlreiche Funktionskennungen). Diese Kennungen haben Zugriffsberechtigungen auf über 6 Millionen Dateien und Verzeichnisse mit einem Volumen von weit über 30 Terabyte. Mit den derzeit zur Verfügung stehenden Standardwerkzeugen ist es kaum möglich exakt festzustellen, auf welche Dateien und Verzeichnisse und mit welchen Rechten (z.B. Lesen, Schreiben, Ändern, Löschen) ein bestimmter Mitarbeiter zugreifen darf bzw. welche Mitarbeiter welche Zugriffsrechte auf eine

bestimmte Datei oder ein bestimmtes Verzeichnis besitzen. Und noch viel weniger ist es möglich, die zeitliche Entwicklung dieser Zugriffsrechte zu verfolgen, weil die Veränderungen durch die Administratoren derzeit nicht automatisch und revisionssicher dokumentiert werden können.

Bislang erfolgt die Administration der Zugriffsrechte jeweils mit der vom Hersteller für den jeweiligen Anwendungszweck mitgelieferten Applikation (die wichtigsten sind dabei Active Directory, Exchange-Server und Netapp-Fileserver). Eine Plattform-übergreifende Verwaltung ist derzeit nicht möglich und die eigentlich notwendige systemübergreifende Transparenz hinsichtlich sämtlicher Berechtigungen eines Benutzers ist nur mit sehr großem Aufwand zu erreichen. Eventuell nicht korrekt erteilte Berechtigungen an Benutzer lassen sich daher nur schwer ermitteln. Zudem sind auf Grund der Vielzahl von Arbeitsschritten in der User-Administration und der gleichzeitig ständig steigenden Komplexität der Anwendungen Fehler nicht vollständig zu vermeiden. Ebenso wenig werden sicherheitsrelevante Zugriffe/Änderungen zur Schaffung von Rechtssicherheit nachvollziehbar mitprotokolliert.

Um den Sicherheitsstandard signifikant zu erhöhen, soll eine zentrale und Plattform-übergreifende Berechtigungsmanagementsoftware zur zentralen Rechte- und Benutzerverwaltung eingeführt werden („*access rights management*“). Ziel ist es dabei zum einen, dass nur autorisierte Personen die IT-Systeme nutzen und auf die für sie relevanten Daten zugreifen können. Zum anderen soll eine zentrale und einheitliche Datenbasis für sämtliche IT-Berechtigungen geschaffen werden, in der neben den aktuellen auch die historisierten Rechte auf Knopfdruck abrufbar sind. Erst mit einem solchen Werkzeug kann die Infrastruktur überwacht und die erstellten Protokoll-dateien können dann mit später auftretenden sicherheitsrelevanten Ereignissen in Zusammenhang gebracht werden. So kann auch auf Hacker-Angriffe schnell und gezielt reagiert werden, bevor ein größerer Schaden entsteht.

In den ersten Monaten nach Einführung eines solchen Werkzeugs ist mit einem Mehraufwand für die Erkennung und die umgehende Korrektur aller nicht passenden Zugriffsrechte zu rechnen. Im Anschluss wird die Pflege der Nutzerdaten (u.a. Anlegen neuer Nutzer, Änderungen, Löschen von Kennungen) dann aber wesentlich effizienter und v.a. sicherer und weniger fehlerbehaftet erfolgen können. Der Sicherheitsstandard kann somit ohne Personalmehrung auf Dauer auf einem erheblich höheren Niveau gehalten werden.

Die geschätzten Investitionskosten liegen bei ca. 140.000.- € (brutto). Hierin enthalten sind Einführungsbegleitung und Schulung sowie 3 Jahre Software-Updates und Telefonsupport. Ab dem Jahr 2019 wird der jährliche Aufwand ca. 25.000 € betragen.