Informationssicherheits- und Datenschutz-Management

STADTVERWALTUNG KOBLENZ

Bericht zur Informationssicherheit

Für die Sitzung des Werkausschusses KGRZ am 11.09.2019

Q2 / 2019

KOBLENZ
VERBINDET.

Wichtige Informationen zu diesem Dokument

Dokumentenklasse:	öffentlich
Dokumententitel:	Bericht zur Informationssicherheit Q2 / 2019
Verantwortliche/r Autor/in:	Merlin Wolf
Dateiname:	2019-09-11_Bericht_Q2_2019
Fassung vom:	28.08.2019
Letzte Veröffentlichung:	28.08.2019
Seitenzahl:	15
freigegeben durch:	Informationssicherheits- und Datenschutz-Management

Impressum

Informationssicherheits- und Datenschutz-Management

STADTVERWALTUNG KOBLENZ
Der Oberbürgermeister

Informationssicherheitsbeauftragter
Schängel-Center, 3. OG, Zimmer 303
Rathauspassage 2
56068 Koblenz

Tel: 0261 / 129 -1263
Fax: 0261 / 129 -1250

Datenschutzbeauftragter
Rathausgebäude II, 1. OG, Zimmer 110
Willi-Hörter-Platz 2
56068 Koblenz

Tel: 0261 / 129 -1214
Fax: 0261 / 129 -1200

E-Mail: security.managment@stadt.koblenz.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Mail Security

Endpoint Security

Vorwort

Die Tatsache, dass weite Bereiche des täglichen Lebens ohne den Einsatz von informationstechnischen Systemen heute nicht mehr funktionsfähig sind, rückt die Frage nach der Sicherheit der Informationen und der Informationstechnologie zunehmend in den Brennpunkt des Interesses. Ein methodisches Sicherheitsmanagement ist zur Gewährleistung umfassender und angemessener Informationssicherheit unerlässlich.

1. Aktuelles im Bereich Informationssicherheit

1.1 ZIDKOR

Als Mitglieder der Arbeitsgruppe INSIDA (Informationssicherheit und Datenschutz) des ZIDKOR (Zweckverband für Informationstechnologie und Datenverarbeitung der Kommunen in Rheinland-Pfalz) unter dem Vorsitz von Herrn Merlin Wolf, erarbeiten die Informationssicherheits- und Datenschutzbeauftragten der Städte Ludwigshafen, Kaiserslautern, Mainz und Koblenz aktuell ein gemeinsames Schulungskonzept für den Bereich Informationssicherheit und Datenschutz.

1.2 Passwortrichtlinie

Aktuell befindet sich eine Richtlinie zum Umgang mit Passwörtern bei der Stadtverwaltung Koblenz in Bearbeitung. Hierbei wird geprüft, ob der turnusmäßige Wechsel von Kennwörtern entfallen kann, wenn die neu eingesetzten Kennwörter eine entsprechende Länge und Komplexität aufweisen. Mit einer Umsetzung der Richtlinie wird in Q4 / 2019 gerechnet.

1.3 Richtlinie zur Entsorgung von Datenträgern

Da die Anforderungen an eine sichere Entsorgung von nicht mehr verwendeten Datenträgern aufgrund der Informationssicherheit und des Datenschutzes stetig zunehmen wurde damit begonnen, für den Bereich der Stadtverwaltung Koblenz eine Richtlinie zur Entsorgung von Datenträgern zu erstellen. In diesem Zusammenhang wird auch die Beschaffung einer zentralen Lösung zum Löschen von Festplatten geprüft. Auch hierfür ist eine Umsetzung in Q4 / 2019 geplant.

1.4 Stellungnahme zur Verwendung von WhatsApp auf dienstlichen Smartphones

Aufgrund einer Anfrage des IT-Managements wurde zum Thema „Verwendung von WhatsApp auf dienstlichen Smartphones“ eine Stellungnahme verfasst. Als Fazit kann mitgeteilt werden, dass für eine dienstliche Nutzung von WhatsApp keine Zustimmung durch das Informationssicherheits- und Datenschutz-Management der Stadtverwaltung Koblenz erteilt wird.

1.5 Schnelle Hilfe für Hosting Kunden des KGRZ

Im Rahmen des Kommunenhostings konnte das KGRZ für einen Kunden eine schnelle Hilfeleistung erbringen und dessen Beitriebsumgebung durch Rückspielen der Datensicherung wiederherstellen, nachdem diese komplett durch eine Verschlüsselungssoftware kompromittiert und verschlüsselt wurde.

2. Gefährdungslage Q2 / 2019

In diesem Bericht wird die Gefährdungslage im Bereich der Informationssicherheit innerhalb der Stadtverwaltung Koblenz und dem Kommunalen Gebietsrechenzentrum Koblenz im Zeitraum vom 01. April 2019 bis 30. Juni 2019 beschrieben.

Der Bericht ist in zwei Bereiche, „Mail Security“ und „Endpoint Security“ unterteilt.

3.1 Mail Security

Heutzutage ist die E-Mail eine der am häufigsten verwendete Kommunikationsform. Um hierbei die notwendige Sicherheit für die Systeme der Stadtverwaltung Koblenz gewährleisten zu können, setzt das Kommunale Gebietsrechenzentrum Koblenz ein Mail-Security System ein, das in der Lage ist, die von Externen eingehende Mails zu analysieren und zu klassifizieren. Hierdurch werden den Mitarbeitern nur die, von dem System als unbedenklich eingestuften E-Mails direkt in deren Postfächer zugestellt.

3.1.1 Gefilterte-Mails

Im 1. Quartal 2019 sind bei der Stadtverwaltung Koblenz insgesamt 591.104 vom Provider KEVAG-Telekom bereits sicherheitstechnisch vorgefilterte E-Mails von externen Absendern eingegangen. Von diesen E-Mails wurden durch die städtischen Sicherheitssysteme noch einmal 337.922 E-Mails herausgefiltert. Der Anteil der sog. „Junk-Mails“, die eine potenzielle Bedrohung für die Systeme der Stadtverwaltung Koblenz darstellten, betrug hiernach 57,17%.

	Zusammensetzung Mails 2019		
	Mails	Echt	Junk
Q2 / 2019	591.104	253.182 (42,83 %)	337.922 (57,17 %)

Abbildung 1Verteilung von Echten-Mails und Junk-Mails

Betrachtet man die Verteilung von „echten Mails“ und „Junk-Mails“ in den jeweiligen Monaten des 2. Quartals 2019 so kann man feststellen, dass die Anzahl an zugestellten Junk-Mails zunahm.

	Zusammensetzung Junk-Mails Q2 / 2019		
	Mails	Echt	Junk
April	184.407	89.173 (48,36 %)	95.234 (51,64 %)
Mai	193.080	86.403 (44,75 %)	106.677 (55,25 %)
Juni	213.617	77.606 (36,33 %)	136.011 (63,67 %)
gesamt	591.104	253.182 (42,83 %)	337.922 (57,17 %)

Abbildung 2 Verteilung von Echten-Mails und Junk-Mails pro Monat in Q2 / 2019

3.1.2 Zusammensetzung der schadhaften Mails

Die von den Systemen des KGRZ als „Junk“ oder herausgefilterten E-Mails setzten sich aus Mails der nachfolgenden Kategorien zusammen:

- Spam[1]
- CM[2]
- DHA[3]
- Phishing[4]
- Richtlinienverletzungen[5]

	Zusammensetzung Junk-Mails 2019						
	Junk	Spam	Virus	Phishing	Richtlinienverletzung	DHA	CM
Q2	337.922	54.208 (16,04 %)	444 (0,13 %)	136 (0,04 %)	6.360 (1,88 %)	19.212 (5,69 %)	257.562 (76,22 %)

Abbildung 3 Zusammensetzung Junk-Mails in Q2 / 2019

In den nachfolgenden Grafiken ist die Aufteilung der gefilterten Mails in die einzelnen oben genannten Kategorien dargestellt:

	Zusammensetzung Junk-Mails 2019						
	Junk	Spam	Virus	Phishing	Richtlinienverletzung	DHA	CM
April	95.234	18.598 (19,53 %)	158 (0,17 %)	30 (0,03 %)	2.228 (2,34 %)	6.667 (7,00 %)	67.553 (70,93 %)
Mai	106.677	19.007 (17,82 %)	203 (0,19 %)	62 (0,06 %)	2.263 (2,12 %)	6.047 (5,67 %)	79.095 (74,14 %)
Juni	136.011	16.603 (12,21 %)	83 (0,06 %)	44 (0,03 %)	1.869 (1,37 %)	6.498 (4,78 %)	110.914 (81,55 %)
gesamt	337.922	54.208 (16,04 %)	444 (0,13 %)	136 (0,04 %)	6.360 (1,88 %)	19.212 (5,69 %)	257.562 (76,22 %)

Abbildung 4 Zusammensetzung Junk-Mails pro Monat in Q2 / 2019

Betrachtet man die Zusammensetzung der „Junk-Mails“ in den einzelnen Monaten des 1. Quartals 2019 so fällt auf, dass sowohl die Anzahl der eingehenden Phishing Mails und der E-Mails - die Viren enthielten - tendenziell abgenommen hat, die Zahl der E-Mails mit schädlichen Viren dennoch weiterhin hoch geblieben ist. Das Gefahrenpotenzial für die Systeme und Daten der Stadtverwaltung Koblenz bleibt daher nach wie vor unverändert hoch.

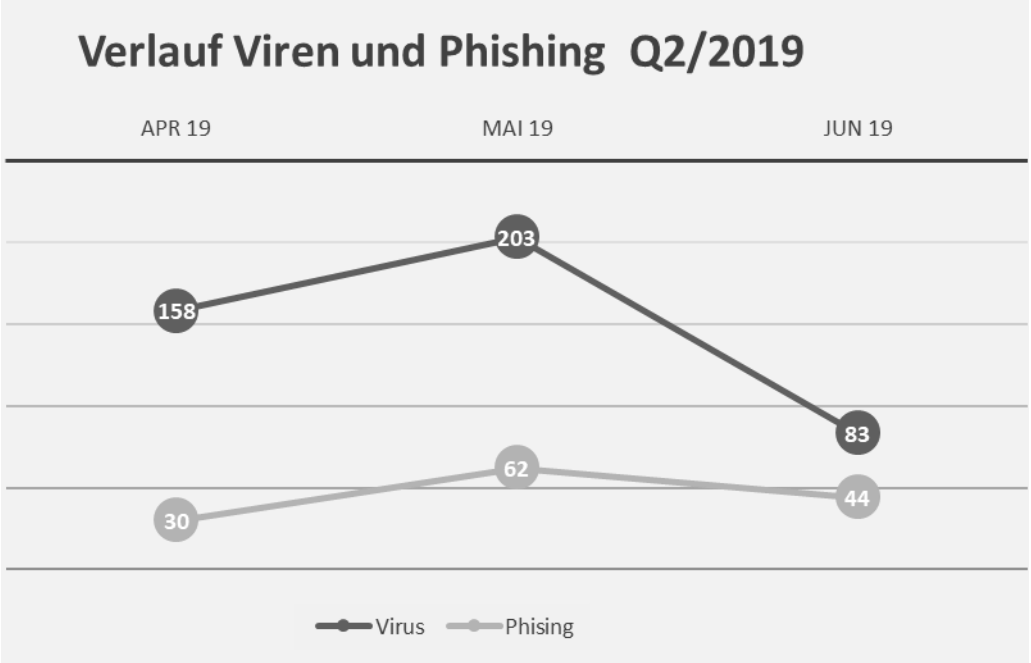

Abbildung 5 Verlauf Viren und Phishing Q2 / 2019

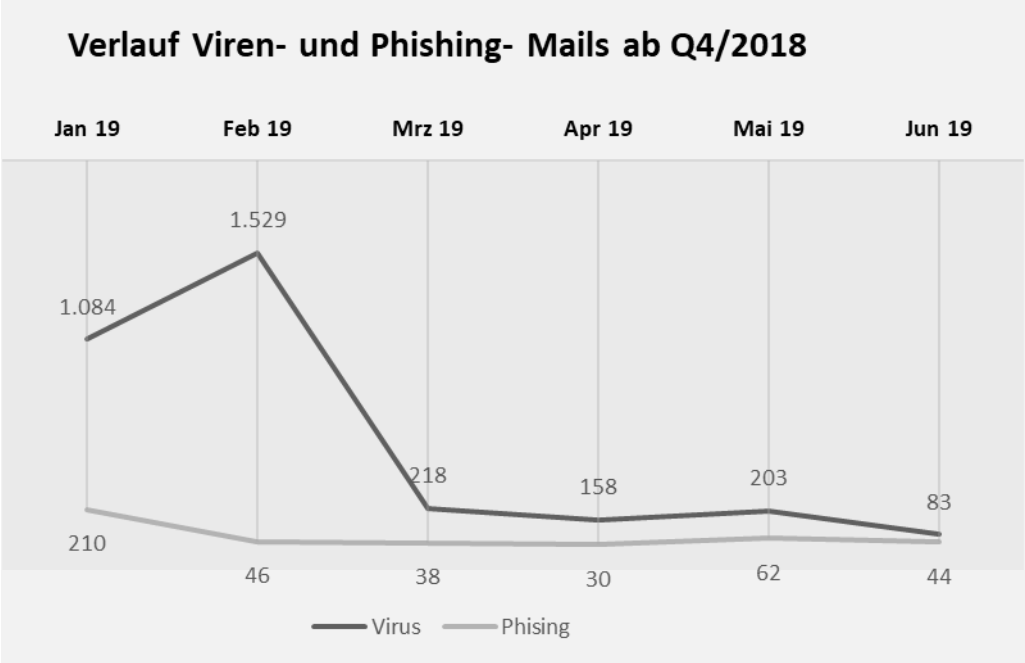

Abbildung 6 Verlauf von Viren und Phishing ab Q4 / 2018

3.2 Endpoint Security

Das Kommunale Gebietsrechenzentrum Koblenz setzt zur Absicherung der Endgeräte wie z. B. Computer, Notebooks etc. mehrere Systeme ein, unter anderem eine IPS[6] (Intrusion Prevention System) und eine Endpoint[7]-Antivirus-Lösung. Beide dienen dazu, Gefahren von den lokalen Systemen im städtischen Netzwerk abzuwehren. Diese können z.B. durch schadhafte E-Mails, unsichere Webseiten oder mobile Datenträger eingeschleust werden.

Die nachfolgenden Grafiken zeigen zum einen die prozentuale Verteilung zwischen Ereignissen des IPS Systems und Endpoint Antivirus Lösung (Malware), als auch die Anzahl der Ereignisse in den einzelnen Monaten des 1. Quartals 2019.

	Zusammensetzung Endpoint 2019		
	Endpoint	Malware	IPS
April	386	44 (11,40 %)	342 (88,60 %)
Mai	281	30 (10,68 %)	251 (89,32 %)
Juni	218	41 (18,81 %)	177 (81,19 %)
gesamt	885	113 (12,99 %)	770 (87,01 %)

Abbildung 7 Anteil von Malware und IPS Ereignissen in Q2 / 2019

Es wird deutlich, dass der größte Anteil an schädlichen Ereignissen bereits durch das IPS System verhindert werden konnte. Darüber hinaus mussten allerdings zusätzlich auch sog. Schadecodes mit einem Anteil von 17% erneut durch den lokalen Virenscanner abgewehrt werden.

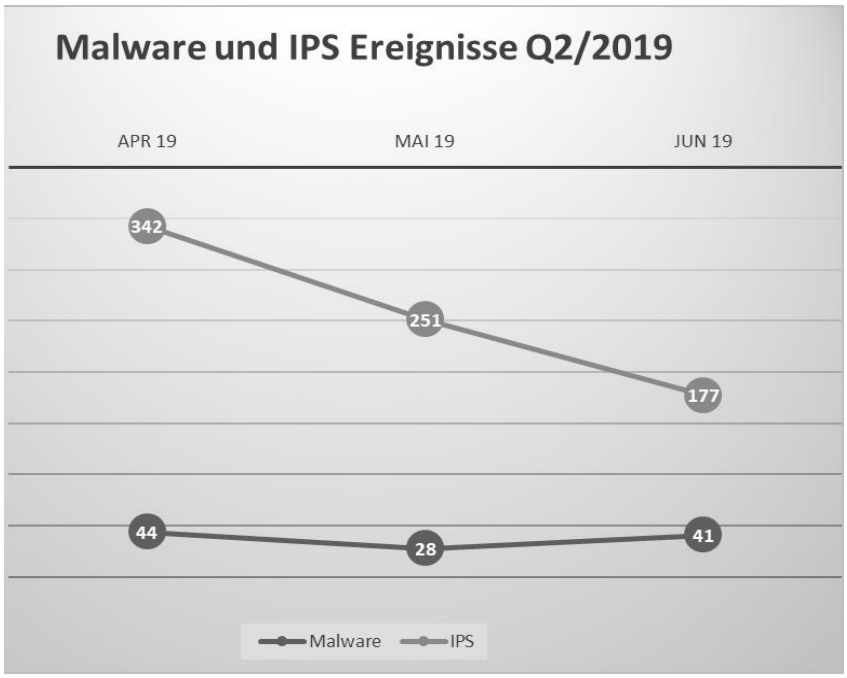

Abbildung 8 Malware und IPS Ereignissen pro Monat in Q2 / 2019

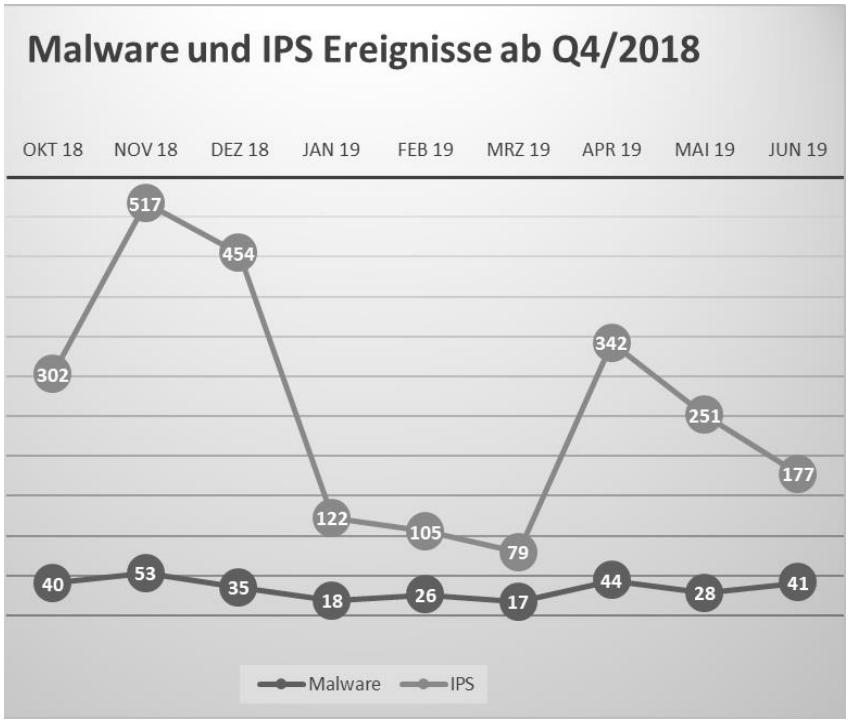

Abbildung 9 Verlauf Malware und IPS Ereignisse ab Oktober 2018

3. Fazit

Bereits im ersten Tätigkeitsbericht 2019 vom 31.01.2019 wurde mit den dort für das Q4/2018 veröffentlichen Zahlen im Bereich der E-Mail- und Endpoint-Sicherheit deutlich, dass die Systeme und Daten der Stadtverwaltung Koblenz täglich einer Vielzahl an Gefährdungen ausgesetzt ist.
In Q1/2019 hatte die Anzahl der Bedrohungen abgenommen. Im dortigen Bericht wurde jedoch bereits drauf hingewiesen, dass erfahrungsgemäß die Gefährdungen immer wieder in Form von sog. „Spam-Wellen“ auftreten und davon auszugehen ist, dass im Verlauf von Q2/2019 mit einem erneuten Anstieg der Bedrohungen zu rechnen ist.

Diese Einschätzung wird nun durch die Zahlen für das Q2 / 2019 bestätigt und zeigt deutlich, dass die Stadtverwaltung Koblenz die vom KGRZ eingeschlagene Strategie im Bereich der Mail- und Endpunkt-Sicherheit als kontinuierlichen Prozess fortschreiben und weiterentwickeln muss. Nur so ist es weiterhin möglich, den täglich neu auftretenden Gefährdungen in einer sinnvollen und wirksamen Weise zu begegnen.

[1] **SPAM**
Als Spam bezeichnet man E-Mails und andere digitale Nachrichten, die für kommerzielle Zwecke unverlangt verschickt werden. Daneben gibt es noch die UCE ("Unsolicited Commercial Electronic Mail") und UBE ("Unsolicited Bulk E-Mail"). Bei letzterer Kategorie handelt es sich nicht unbedingt um E-Mails zu kommerziellen Zwecken, sondern um jegliche E-Mails, die massenweise unerwünscht versendet werden. E-Mails zu Werbezwecken, die ein Kunde nach dem Ankauf eines Produktes von dem Verkäufer erhält, werden in der Regel nicht als Spam gerechnet. Oft sind Spam-E-Mails einfach nur lästig. Doch sie können auch gefährlich sein, wenn sie zum Beispiel Daten des Users erfragen.

[2] **CM**

Eingehenden E-Mails die an eine Mailadresse gesendet werden, die nicht auf dem Mailserver der Stadtverwaltung Koblenz existiert, werden automatisch abgelehnt und der Absender mit dem Fehlercode 550 benachrichtigt. E-Mails die von einem Absender versendet werden, dessen IP-Adresse auf der Seite Spamhouse.org gelistet ist, wird ebenfalls zurückgesendet und nicht zugestellt.

[3] **DHA**

Ein Directory-Harvest-Angriff (DHA) ist ein Versuch, die mit einem E-Mail-Server zusammenhängenden gültigen Adressen zu identifizieren, sodass sie in eine Spam-Datenbank eingefügt werden können. Ein Directory-Harvest-Angriff kann eine von zwei Methoden zum Sammeln der gültigen E-Mail-Adressen verwenden. Die erste Methode basiert auf Brute-Force und sendet eine Nachricht an alle möglichen alphanumerischen Kombinationen bis zu einer Länge von n (wo „n" eine voreingestellte positive Zahl wie beispielsweise 15 ist), die vom Server als Benutzerabschnitt der E-Mail-Adresse verwendet werden könnten. Bei der zweiten und selektiveren Methode wird eine Nachricht an die wahrscheinlichsten Benutzernamen gesendet – beispielsweise alle möglichen Kombinationen von Initialen gefolgt von gängigen Nachnamen. In beiden Fällen sendet der E-Mail-Server in der Regel eine „Adresse nicht gefunden" Nachricht zurück, falls die Adresse nicht existiert, aber keine Nachricht für E-Mails, die an gültige Adressen übertragen wurden. Das DHA-Programm erstellt eine Datenbank aller E-Mail-Adressen am Server, die während des Angriffs nicht zurückgemeldet wurden.

Der DHA-Ansatz erklärt auch, wie eine neue E-Mail-Adresse bereits Tage oder Stunden nach dem Anlegen gespammt werden kann. Verschiedene Lösungen wurden entwickelt, um Angriffe dieser Art zu bekämpfen. Die effektivsten Methoden verlangsamen die Geschwindigkeit, mit welcher der Angriff stattfinden kann, statt den Angriff herausfiltern zu wollen. Dazu kann man die Anzahl der eingehenden E-Mail-Nachrichten pro Minute oder Stunde einschränken, ob legitim oder Spam. So genannte Spamfilter, die dafür programmiert sind, bestimmte für Spam typische Zeichen- und Wortkombinationen zu erkennen, können auch wirksam sein, obwohl sie manchmal auch legitime Nachrichten zurückweisen.

[4] **Phishing**

Phishing ist ein von dem englischen Wort „fishing" abgeleiteter Begriff, der ins Deutsche übersetzt Angeln oder Fischen bedeutet. Der Begriff verdeutlicht bildlich, um was es geht: das betrügerische Angeln oder Fischen von sensiblen Daten wie Passwörter mithilfe verschiedener Köder im Internet.

In der Regel liegt das Augenmerk der Phisher auf Zugangsdaten für Onlinebanking-Accounts oder Informationen von Kreditkarten.

Dabei ist das Phishing ein ziemlich erfolgreiches Prinzip. Bei einer Phishing-Aktion klicken mehr als zehn Prozent aller Internetnutzer, die im Fokus einer solchen Attacke stehen, auf einen schädlichen Link oder öffnen einen gefährlichen Anhang. Das bedeutet, ein Betrüger muss zum Beispiel 10 E-Mail-Nachrichten verschicken, um mit höchster Wahrscheinlichkeit einen Nutzer zu finden, von dem er die persönlichen Daten erbeutet.

[5] **Richtlinienverletzungen**

Bei der Stadtverwaltung Koblenz wurde festgelegt, dass alle E-Mail die eines der folgenden Datenformate als Anhang beinhaltet blockiert werden: Word, Excel, PowerPoint und Rar Formate.

[6] **IPS**

Ein Intrusion Prevention System, abgekürzt IPS, ist in der Lage, Angriffe auf Netzwerke oder Computersysteme zu erkennen und automatische Abwehrmaßnahmen zu ergreifen. Es sorgt gegenüber herkömmlichen Firewall-Systemen für einen zusätzlichen Schutz.

[7] **Endpoint Antivirus**

Ist der lokal installierte Virenscanner, er überwacht zunächst den laufenden Datenverkehr auf bösartige Software. Dadurch wird jedes Programm und jede Mail gescannt, bevor man sie herunterlädt. Wird ein verdächtiger Code gefunden, wird der Virus automatisch entfernt.