Informationssicherheits- und Datenschutz-Management
STADTVERWALTUNG KOBLENZ

Bericht zur Informationssicherheit

Für die Sitzung des Werkausschusses KGRZ am 29.05.2019

Tätigkeitsbericht Q1 / 2019

KOBLENZ
VERBINDET.

Wichtige Informationen zu diesem Dokument

Dokumentenklasse:	öffentlich
Dokumententitel:	Bericht zur Informationssicherheit Q1 / 2019
Verantwortliche/r Autor/in:	Merlin Wolf
Dateiname:	2019-04-01_Bericht_Q1_2019
Fassung vom:	01.04.2019
Letzte Veröffentlichung:	29.05.2019
Seitenzahl:	16
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. Informationssicherheit

1.2 Umgesetzte Maßnahmen

1.2.1 Umsetzung der Anforderungen des neuen Grundschutzes

Das neue IT-Grundschutzkompendium unterliegt einer stetigen Anpassung durch das BSI. Dies wiederum bedingt eine fortlaufende und andauernde Analyse sowie Umsetzung der neuen Anforderungen.

1.2.2 Empfehlung für eine neue Fernwartungssoftware

Vor dem Hintergrund, dass die sich aktuell im KGRZ im Einsatz befindliche Fernwartungslösung (PC-Visit) einen relativ hohen personellen Ressourceneinsatz erfordert, wurde das Informationssicherheits- und Datenschutz- Management durch das KGRZ gebeten, die in Frage kommende neue Lösung (Team-Viewer) auf die Anforderungen der Informationssicherheit und des Datenschutzes hin zu prüfen. Dem KGRZ wurde nach eingehender Prüfung eine Freigabe der gewünschten Software erteilt. Vor dem Einsatz ist jedoch noch ein entsprechendes Fernwartungskonzept mit den entsprechenden Richtlinien zu erstellen.

1.3 Andauernde Maßnahmen

1.3.1 Umsetzung der Anforderungen des neuen Grundschutzes

Wie unter 1.2.1 bereits erwähnt, werden die neuen Anforderungen fortlaufend analysiert und sukzessive umgesetzt. Im Februar 2019 wurde die 2. Edition des IT-Grundschutzkompendiums veröffentlicht, welche weitere neue Bausteine zur Umsetzung bereitstellt.

1.3.2 Abstimmungsgespräche

Es findet weiterhin eine enge Zusammenarbeit mit dem IT-Management der Stadtverwaltung Koblenz statt. Hierzu finden 14 tägige Besprechungen mit Beteiligung der Werkleitung des KGRZ statt, um grundlegende Fragestellungen der Informationssicherheit zu erörtern und ggf. Projekte zu Themen im Bereich der Informationssicherheit zu initiieren und zu überwachen.

2. Gefährdungslage Q1 / 2019

In diesem Bericht wird die Gefährdungslage im Bereich der Informationssicherheit innerhalb der Stadtverwaltung Koblenz und dem Kommunalen Gebietsrechenzentrum Koblenz im Zeitraum vom 01. Januar 2019 bis 31. März 2019 beschrieben.

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

2.1 Mail Security

In der heutigen Zeit ist E-Mail eine der am häufigsten verwendeten 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 eingestufte E-Mails direkt in deren Postfächer zugestellt.

2.1.1 Gefilterte-Mails

Im 1. Quartal 2019 sind bei der Stadtverwaltung Koblenz insgesamt 527.533 vom Provider Kevag-Telekom bereits sicherheitstechnisch vorgefilterte E-Mails von externen Absendern eingegangen. Von diesen E-Mails wurden durch die eingesetzten Sicherheitssysteme 262.115 E-Mails herausgefiltert. Der Anteil der sog. „Junk-Mails“, die eine potenzielle Bedrohung für die Systeme der Stadtverwaltung Koblenz darstellten, betrug hiernach 50%.

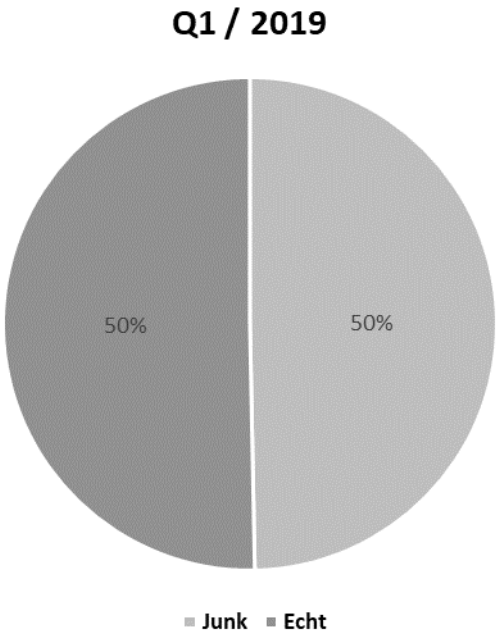

Abbildung 1 Verteilung von Echten –Mails und Junk-Mails

Betrachtet man die Verteilung von „echten Mails“ und „Junk-Mails“ in den jeweiligen Monaten des 1. Quartals 2019 so kann man feststellen, dass die Anzahl an zugestellten Junk-Mails tendenziell eher zunahm.

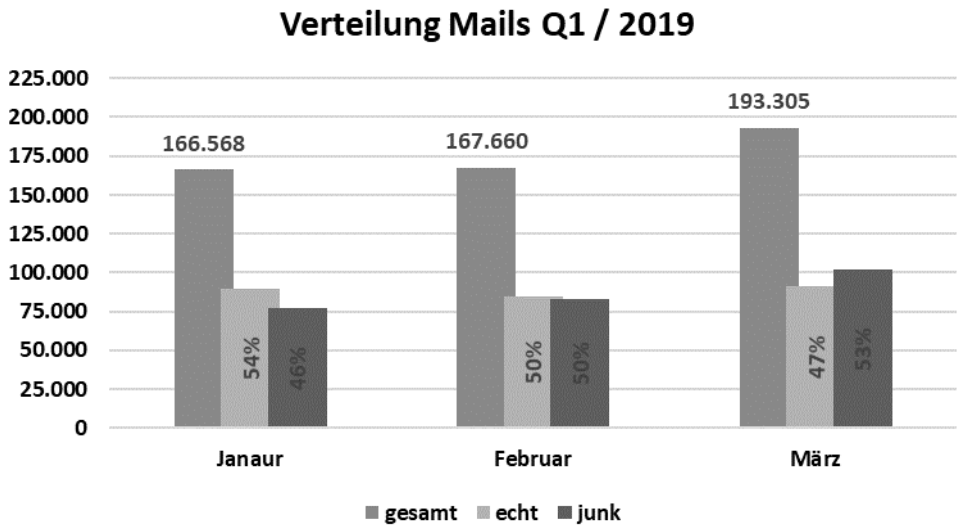

Abbildung 2 Verteilung von Echten-Mails und Junk-Mails pro Monat in Q1 /2019

2.1.2 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]

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

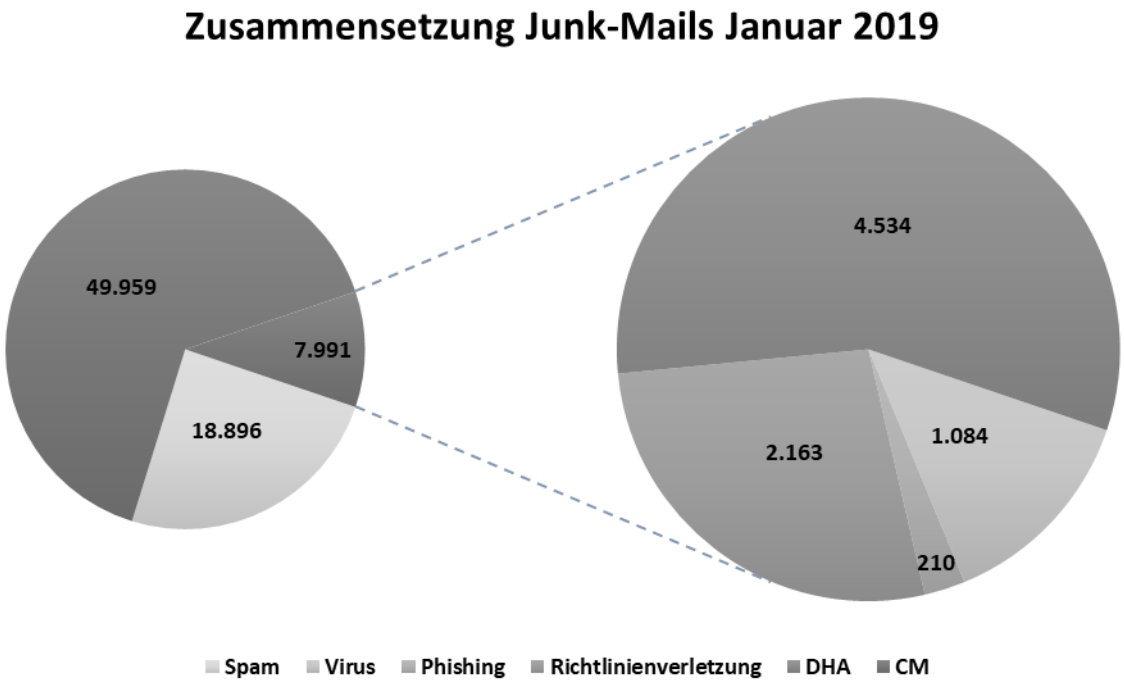

Abbildung 3 Zusammensetzung der Junk-Mails Januar 2019 nach Kategorien

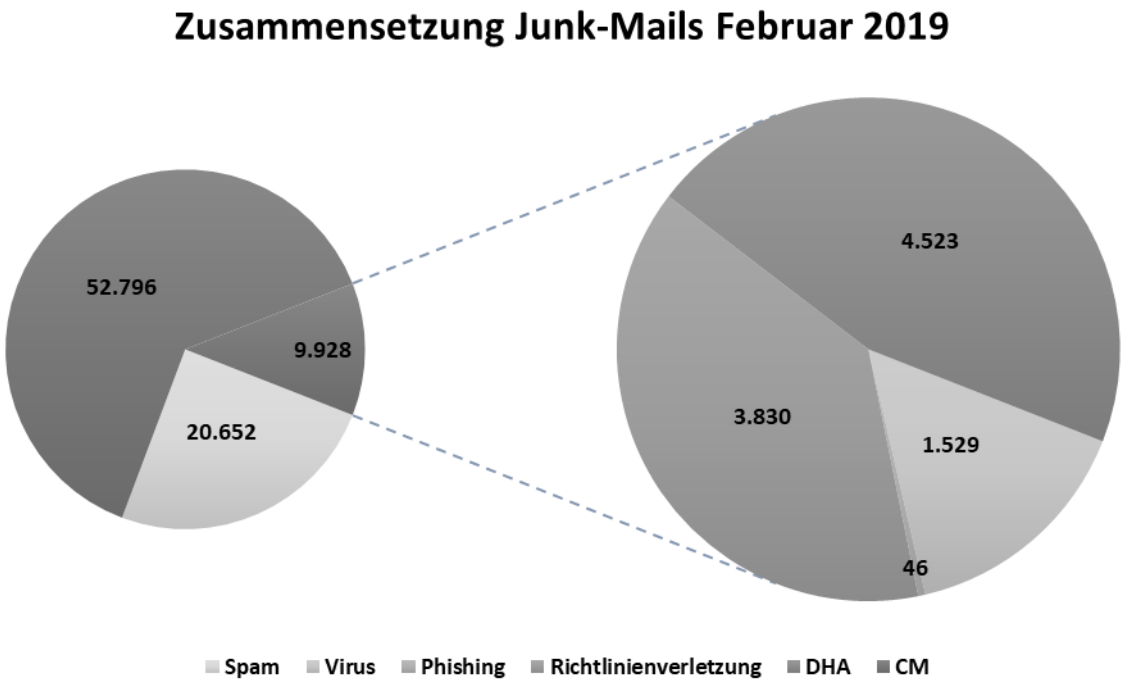

Abbildung 4 Zusammensetzung der Junk-Mails Februar 2019 nach Kategorien

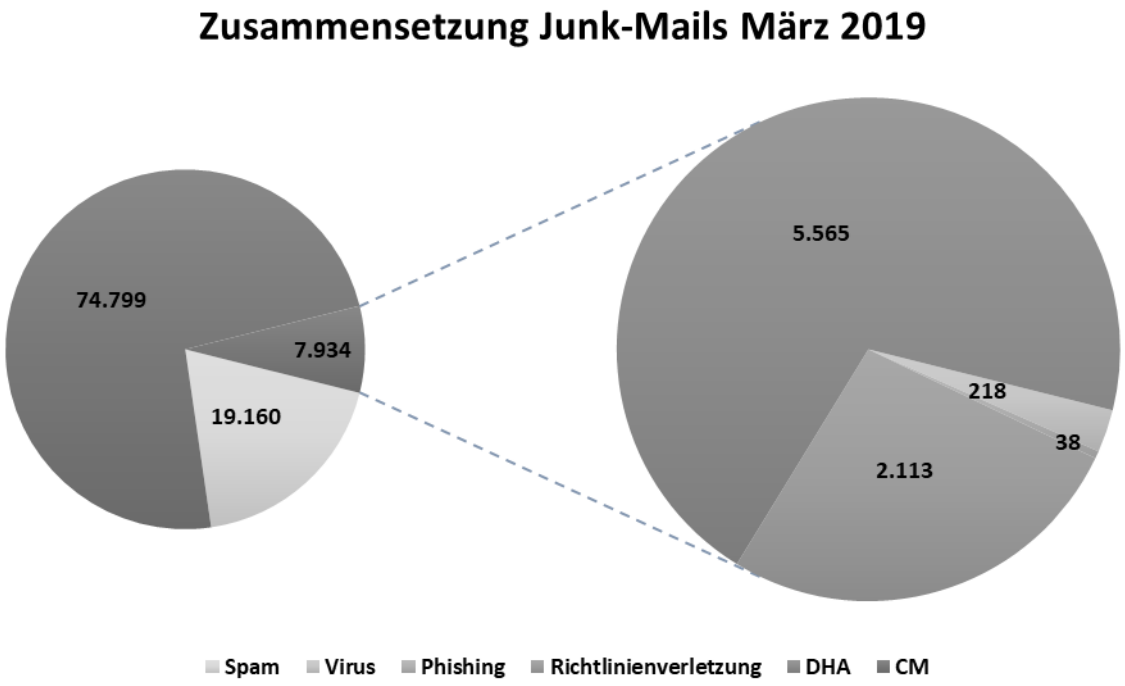

Abbildung 5 Zusammensetzung der Junk-Mails März 2019 nach Kategorien

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 und ein Gefahrenpotenzial für die Systeme und Daten der Stadtverwaltung Koblenz nach wie vor fortbesteht.

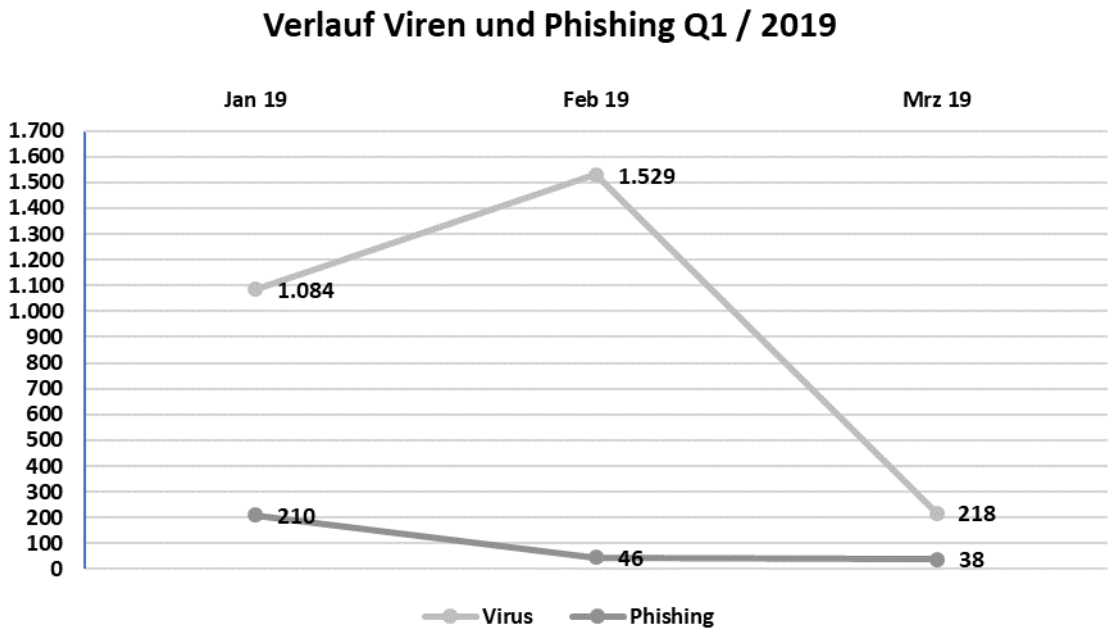

Abbildung 6 Verlauf Viren und Phishing Q1 / 2019

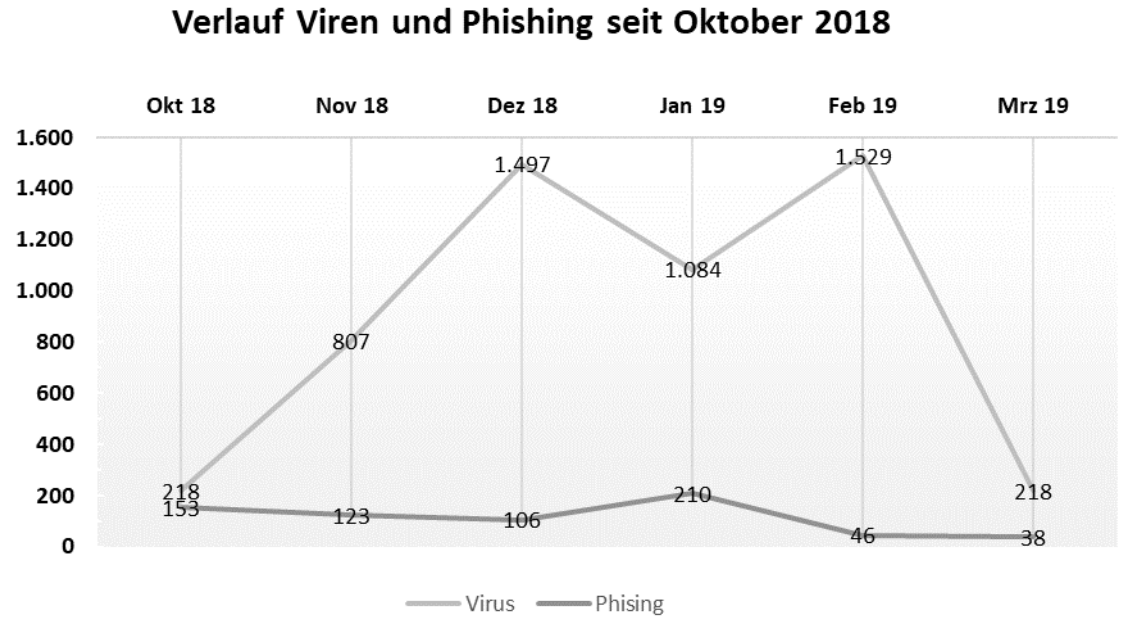

Abbildung 7Verlauf von Viren und Phishing seit Oktober 2018

2.2 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.

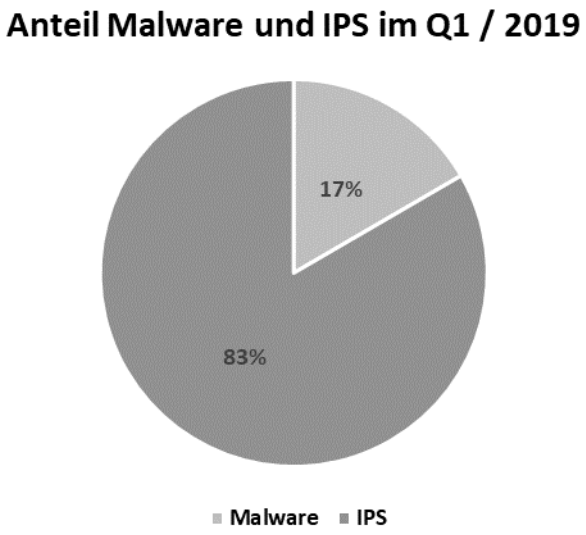

Abbildung 8 Anteil von Malware und IPS Ereignissen in Q1 / 2019

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

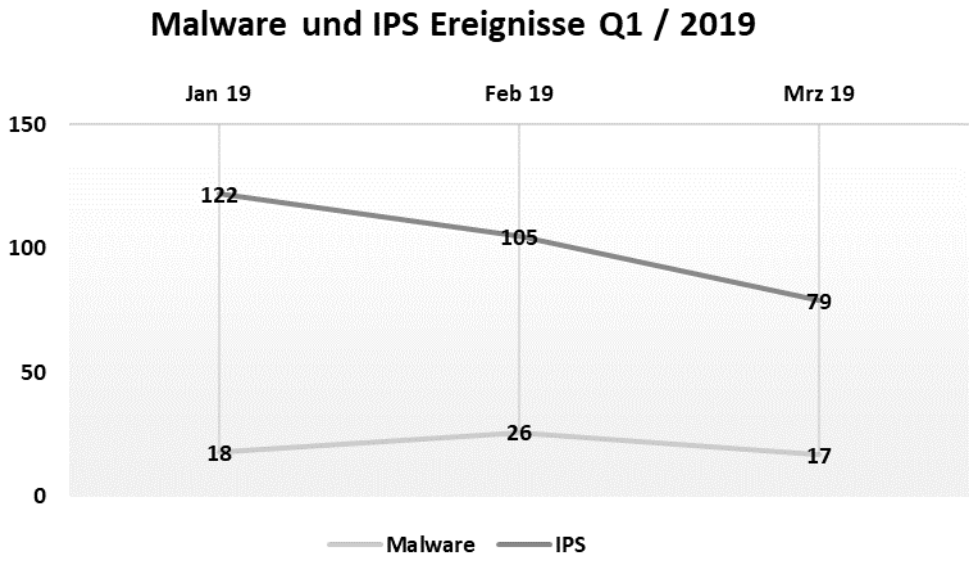

Abbildung 9 Verteilung von Malware und IPS Ereignissen pro Monat in Q1 / 2019

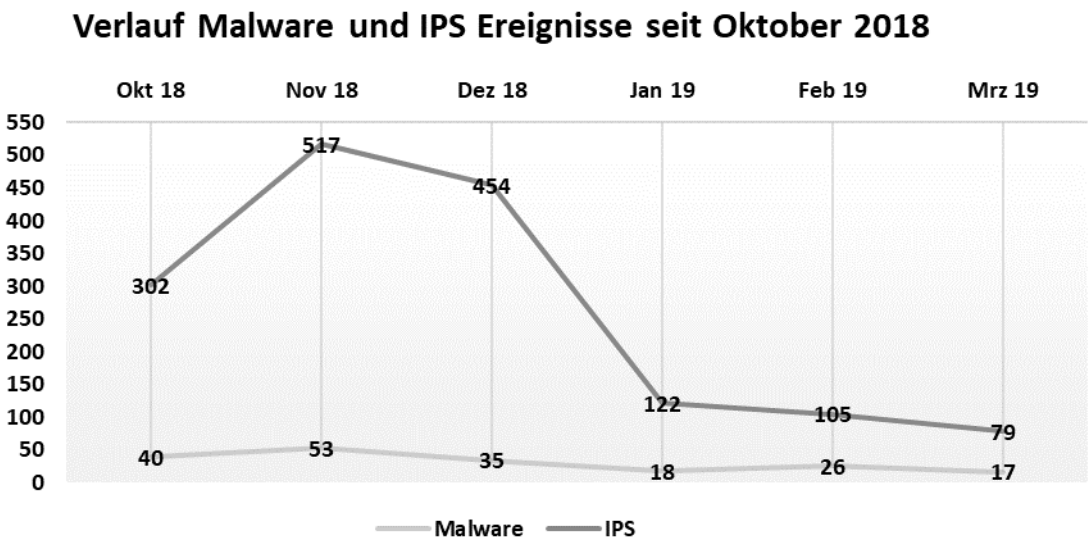

Abbildung 10 Verlauf Malware und IPS Ereignisse seit Oktober 2018

3 Fazit

Bereits im Ersten Tätigkeitsbericht 2019 vom 31.01.2019 wurde mit den dort zum ersten Mal 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 hat die Anzahl der Bedrohungen abgenommen. Erfahrungsgemäß treten die Gefährdungen aber in Form von sog. „Spam-Wellen“ auf.
Es ist daher davon auszugehen, dass im Verlauf von Q2/2019 wieder mit einem Anstieg aufgrund einer neuen „Spam-Welle“ zu rechnen ist.
Dies geht u. a. auch aus dem Lagebericht 2018 des Bundesamtes für Sicherheit in der Informationstechnik hervor, in dem ein Anstieg an Schadprogrammen festgestellt wird. Danach gibt es über 800 Millionen bekannte Schadprogramme. Pro Tag kommen rund 390.000 neue Varianten hinzu.

Daher ist es besonders wichtig, dass die vom KGRZ gewählte Strategie im Bereich der Mail- und Endpunkt-Sicherheit weiter ausgebaut wird. Ohne die aktuell eigesetzten Systeme wäre die Stadtverwaltung Koblenz einem viel höheren Risiko ausgesetzt, Opfer eines Angriffes durch Dritte zu werden.

Aus diesem Grund wurde dem Kommunalen Gebietsrechenzentrum durch das Informationssicherheits- und Datenschutz-Management vorgeschlagen, sich mit dem Thema ReCoBS (Remote-Controlled Browser System) für ein sicheres Surfen im Internet zu beschäftigen. Aktuell wird dieses Thema konzeptionell im KGRZ aufbereitet.

[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.