Informationssicherheits- und Datenschutz-Management
STADTVERWALTUNG KOBLENZ

Bericht zur Informationssicherheit

Für die Sitzung des Werkausschusses KGRZ am 14.02.2019

Tätigkeitsbericht Q4 / 2018

vom 31.01.2019

KOBLENZ
VERBINDET.

Wichtige Informationen zu diesem Dokument

Dokumentenklasse:	nicht öffentlich
Dokumententitel:	Bericht zur Informationssicherheit Q4 / 2018
Verantwortliche/r Autor/in:	Merlin Wolf
Dateiname:	2019-01-31_Bericht_Q4_2018
Fassung vom:	31.01.2019
Letzte Veröffentlichung:	31.01.2019
Seitenzahl:	18
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. Organisatorisches

1.1 Berichtswesen

Um den Mitgliedern des Werkausschuss KGRZ einen Überblick über die Lage der Informationssicherheit sowohl im KGRZ als auch in der Stadtverwaltung Koblenz bieten zu können, wird das Berichtswesen wir folgt aufgebaut:

Quartalsbericht

Immer zur Mitte des aktuellen Quartals wird ein Bericht über die Lage der Informationssicherheit erstellt. Dieser Bericht umfasst dann die Ereignisse / Tätigkeiten des vorangegangenen Quartals.
D.h., in Q1/2019 sind im Bericht die Ereignisse / Tätigkeiten des Q4/2018 enthalten.

Jahresbericht

Immer zur Mitte des ersten Quartals eines Jahres wird ein Bericht zur Lage der Informationssicherheit erstellt; dieser umfasst das voran gegangene Jahr. Der erste Jahresbericht zur Informationssicherheit wird daher in Q1/2020 erscheinen.

2. Informationssicherheit im KGRZ

2.2 Umgesetzte Maßnahmen

2.2.1 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.

2.2.2 Richtlinie zum Sicherheitsvorfallmanagement

Eine der zentralen Aufgaben des Informationssicherheitsmanagements ist das Erfassen von Sicherheitsvorfällen und die Dokumentation der getroffenen Gegenmaßnahmen. Hierzu wurde am 15.12.2018 die Richtlinie zum Sicherheitsvorfallmanagement (SVMRL) veröffentlicht und den Mitarbeitern des KGRZ zur Verfügung gestellt.

2.3 Andauernde Maßnahmen

2.3.1 Umsetzung der Anforderungen des neuen Grundschutzes

Wie unter 2.2.1 bereits erwähnt, werden die neuen Anforderungen fortlaufend analysiert und sukzessive umgesetzt. Im Februar 2019 wird die 2. Edition des IT-Grundschutzkompendiums veröffentlicht, welche weitere neue Bausteine zur Umsetzung bereitstellt.

2.3.2 Sichereres Rechenzentrum (KGRZ.SRZ)

Mit der Prüfung der im neuen Rechenzentrum (KGRZ.SRZ) umgesetzten Maßnahmen hinsichtlich der Einhaltung aktueller IT-Grundschutz-Anforderungen wurde inzwischen begonnen. Allerdings hat das BSI zwischenzeitlich im Rahmen der jüngsten Überarbeitung des IT-Grundschutzkompendiums für den Bereich der Rechenzentren einen neuen, separaten Baustein (INF.2 Rechenzentrum sowie Serverraum CD vom 22.11.2018) konkretisiert. Aktuell werden die Prüfpunkte des neuen Bausteins in die Prüfung übernommen und abgearbeitet. Hiernach kann die Prüfung des sicheren Rechenzentrums als Hülle zur Erbringung der Services abgeschlossen werden.

3. Informationssicherheit in der Stadtverwaltung

3.1 Umgesetzte Maßnahmen

3.1.1 Neustart von Rechnern aufgrund von Bedrohungslagen

Anfang dieses Jahres wurden die Kolleginnen und Kollegen der Stadtverwaltung Koblenz darüber informiert, dass aufgrund der aktuellen bzw. andauernden Bedrohungslage, zukünftig ein Neustart von Rechnern durch das KGRZ erzwungen werden kann/wird.

Diese Sicherheitsmaßnahme ist leider notwendig, da – entgegen der Vorgabe durch das KGRZ – immer noch viele Rechner nach Dienstende nicht heruntergefahren und am Folgetag wieder neugestartet werden. Dieses Vorgehen ist allerdings zwingend erforderlich, damit wichtige Sicherheitsupdates automatisch eingespielt und der andauernden Bedrohungslage unter anderem auf diese Weise entgegnet werden kann.

3.1.2 Informationssicherheitsleitlinie

Nachdem bereits zum 01.01.2018 die Informationssicherheitsleitlinie für das Kommunale Gebietsrechenzentrum Koblenz in Kraft getreten ist, wurde nun die Informationssicherheitsleitlinie für die Stadtverwaltung Koblenz verfasst und soll in Q1/2019 in Kraft treten und veröffentlicht werden.

3.2 Wiederkehrende Maßnahmen

Es findet 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.

4. Gefährdungslage

In diesem Bericht wird die Gefährdungslage im Bereich der Informationssicherheit innerhalb der Stadtverwaltung Koblenz und dem Kommunalen Gebietsrechenzentrum Koblenz im Zeitraum vom 01. Oktober 2018 bis 31. Dezember 2018 beschrieben.

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

4.1 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, dass 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.

4.1.1 Gefilterte-Mails

Im 4. Quartal 2018 sind bei der Stadtverwaltung Koblenz insgesamt 561.845 E-Mails von externen Absendern eingegangen. Von diesen E-Mails wurden durch die angewendeten Sicherheitssysteme 319.482 E-Mails herausgefiltert. Der Anteil der sog. „Junk-Mails“, die eine potenzielle Bedrohung für die Systeme der Stadtverwaltung Koblenz darstellten, betrug hiernach 57%.

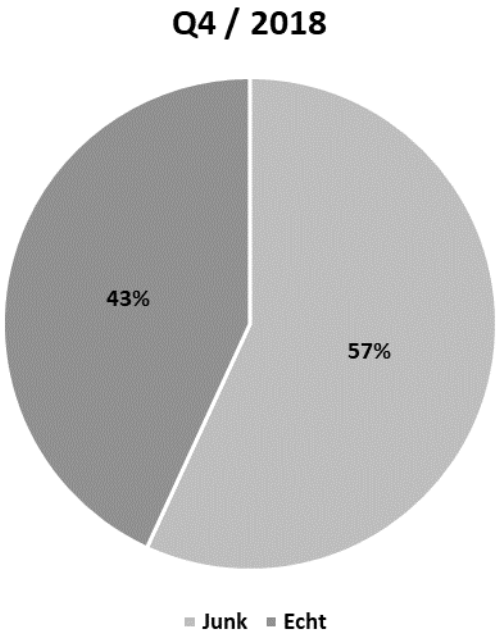

Abbildung 1 Verteilung von Echten –Mails und Junk-Mails

Betrachtet man die Verteilung von „echten Mails“ und „Junk-Mails“ in den jeweiligen Monaten des 4. Quartals 2018 so kann man feststellen, dass die Anzahl an zugestellten Junk-Mails tendenziell eher zunahm.

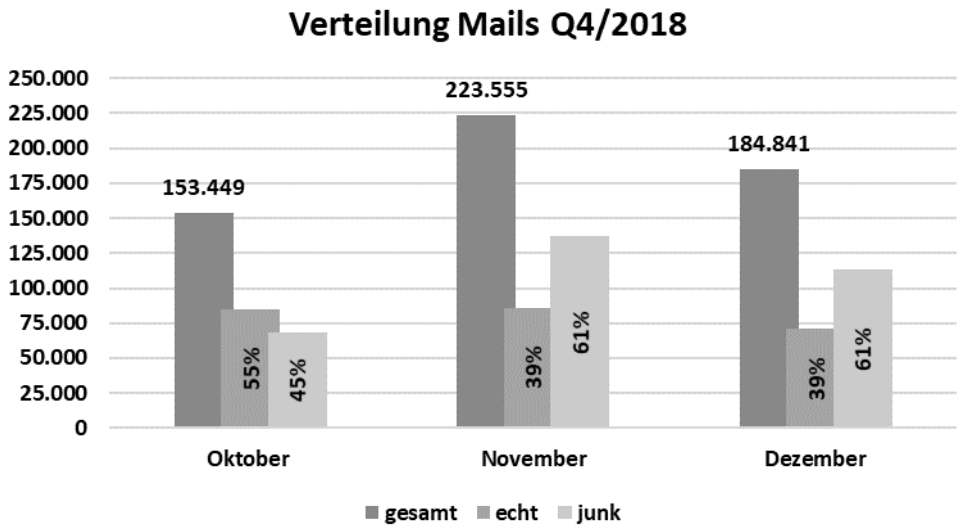

Abbildung 2 Verteilung von Echten-Mails und Junk-Mails pro Monat in Q4 /1028

4.1.2 Zusammensetzung der Spam-Mails

Die von den Systemen des KGRZ als „Spam“ 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:

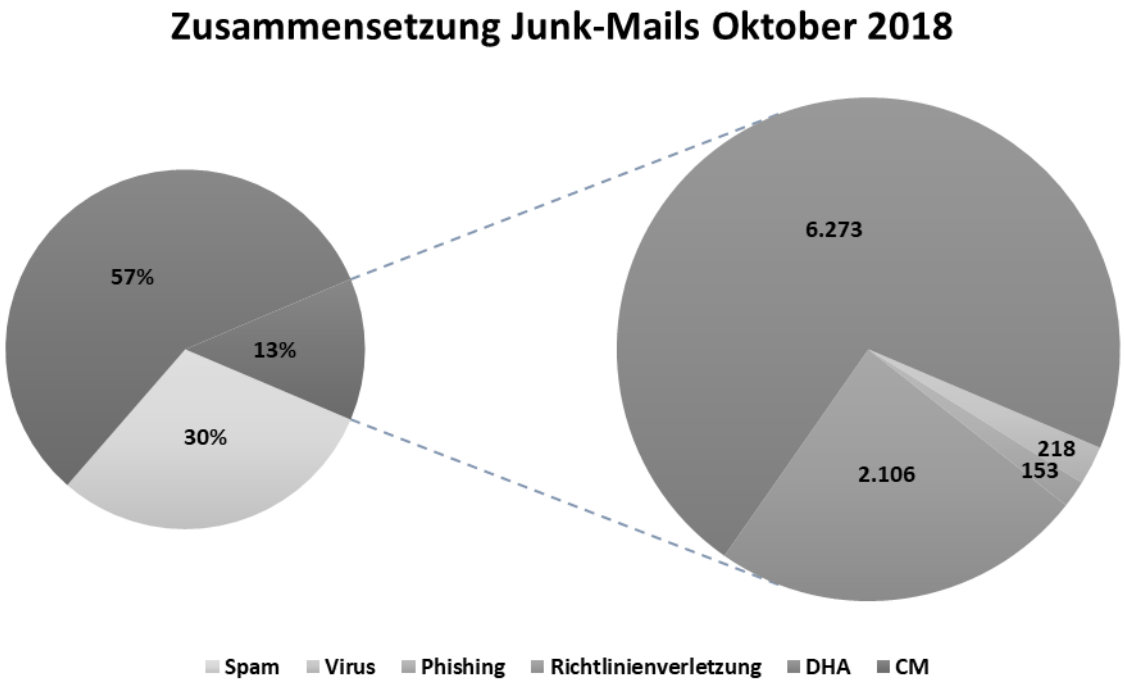

Abbildung 3 Zusammensetzung der Junk-Mails Oktober 2018 nach Kategorien

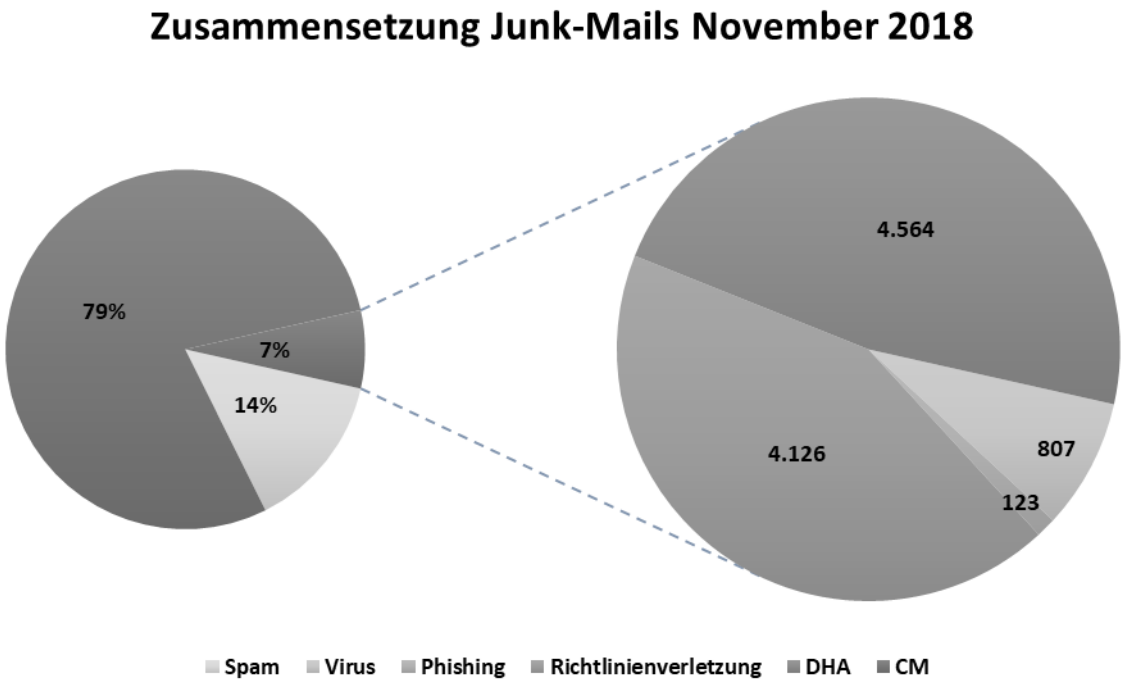

Abbildung 4 Zusammensetzung der Junk-Mails November 2018 nach Kategorien

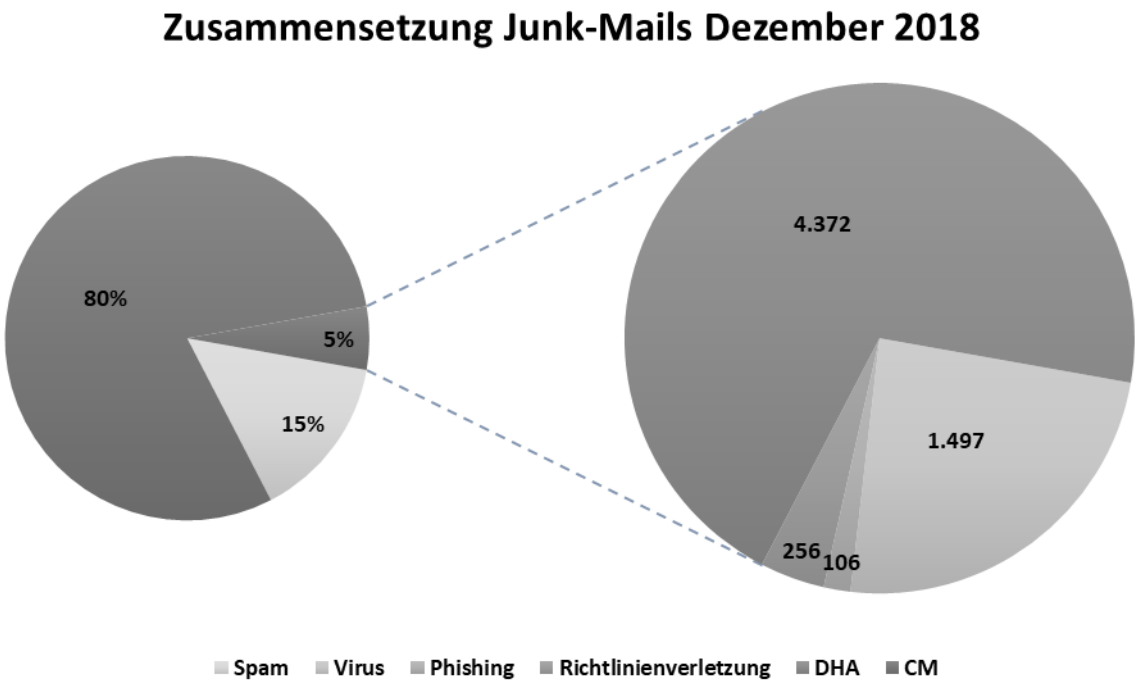

Abbildung 5 Zusammensetzung der Junk-Mails Dezember 2018 nach Kategorien

Betrachtet man die Zusammensetzung der „Junk-Mails“ in den einzelnen Monaten des 4. Quartals 2018 so lässt sich feststellen, dass zwar die Anzahl der eingehenden „Phishing Mails“ ab, die Zahl der E-Mails aber, die Viren enthielten und somit den Systemen der Stadtverwaltung Koblenz gefährlich werden konnten, zunahm.

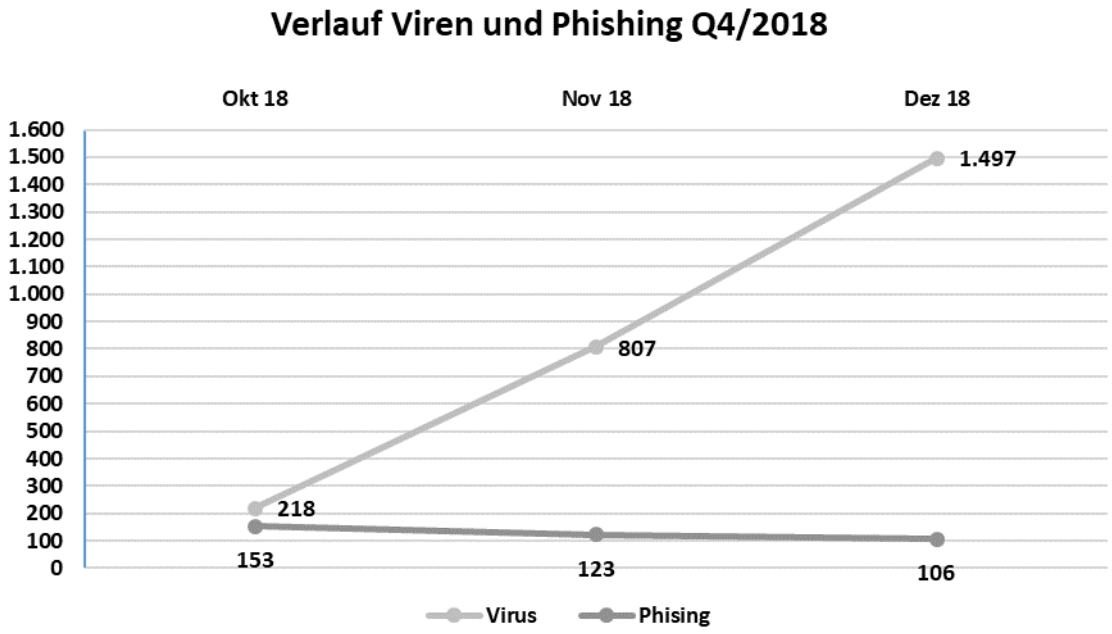

Abbildung 6 Verlauf Viren und Phishing Q4 /1028

4.2 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 ein. Beide dienen dazu, Gefahren von den lokalen Systemen im städtischen Netzwerk abzuwehren.

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 4. Quartals 2018.

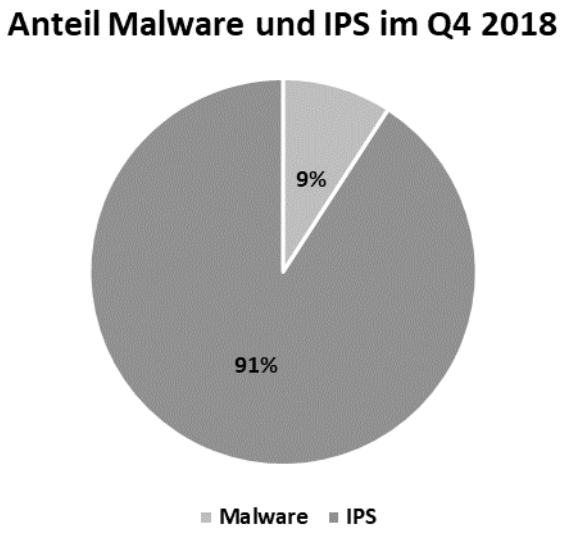

Abbildung 7 Anteil von Malware und IPS Ereignissen in Q4 / 2018

Es wird deutlich, dass der größte Anteil an schädlichen Ereignissen bereits durch das IPS System verhindert werden konnte, nur ein kleiner Anteil von 9% an Schadecode musste noch durch den lokalen Virenscanner abgewehrt werden.

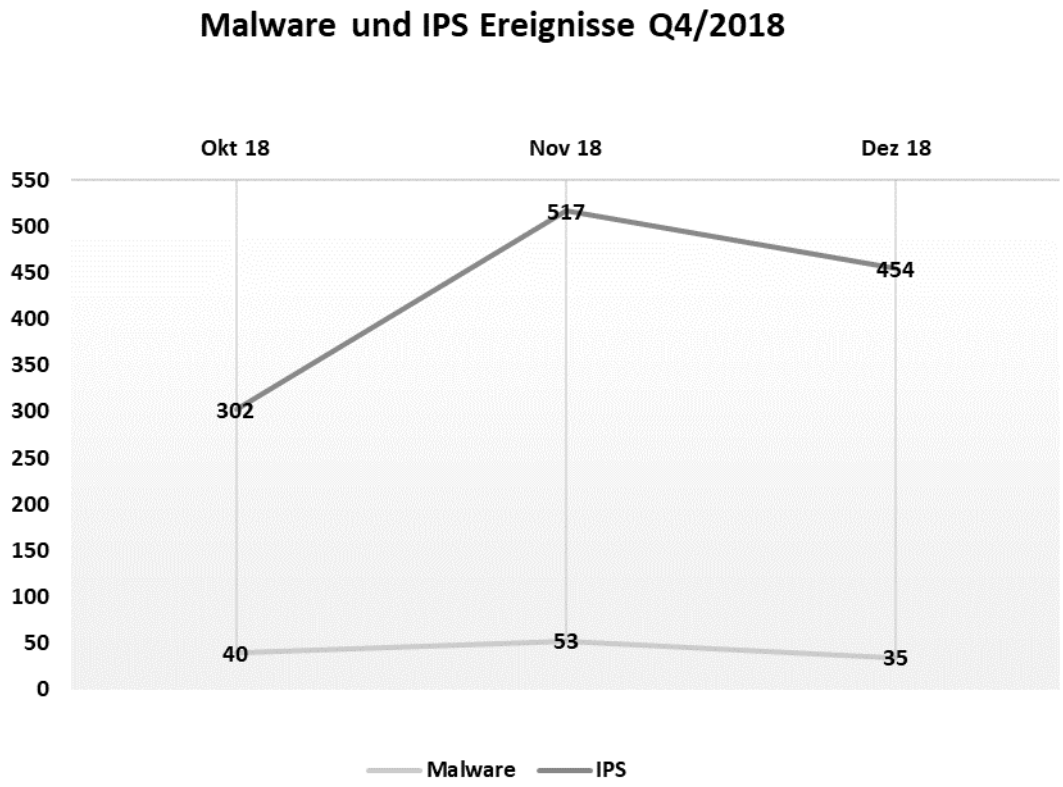

Abbildung 8 Verteilung von Malware und IPS Ereignissen pro Monat in Q4 / 2018

5 Fazit

Anhand der in diesem Bericht zum ersten Mal veröffentlichen Zahlen im Bereich der E-Mail- und Endpoint-Sicherheit lässt sich sehr gut erkennen, dass die Anzahl der Bedrohungen tendenziell nicht ab-, sondern “sehr“ wahrscheinlich eher zunimmt.
In seinem Lagebericht 2018 teilt das Bundesamt für Sicherheit in der Informationstechnik mit, dass insgesamt die Anzahl an Schadprogrammen weiter gestiegen ist; es gibt über 800 Millionen bekannte Schadprogramme. Pro Tag kommen rund 390.000 neue Varianten hinzu.

Gleichzeitig befinden wir uns erst am Anfang einer Ära der Digitalisierung in der öffentlichen Verwaltung, die unseren Alltag beeinflussen wird. Angriffe und Gefährdungen, die das Kommunale Gebietsrechenzentrum bereits heute vor extreme Herausforderungen stellen, werden in einer digitalisierten und vernetzten Verwaltung weiter zunehmen.

Ohne entsprechende Anstrengungen, das notwendige Maß an Informationssicherheit durch Prävention, Detektion und Reaktion zu gewährleisten, wird die Verwaltung zunehmend gefährdet.

Das Problem liegt in der Kombination von wachsender Gefährdung mit einer zunehmenden Abhängigkeit von der eingesetzten Informationstechnik. Die Wahrscheinlichkeit für den Erfolg von Angriffen auf digitalisierte Infrastrukturen steigt, da sich die Anzahl der Angriffspunkte erhöht, die Kommunikationsinfrastrukturen immer komplexer werden und die zu verarbeitenden Datenmengen sich vervielfachen.

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.

[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.