Informationssicherheits- und Datenschutz-Management

STADTVERWALTUNG KOBLENZ

Bericht zur Informationssicherheit

Für die Sitzung des Werkausschusses KGRZ am 05.02.2020

2. Halbjahr / 2019

KOBLENZ
VERBINDET.

Wichtige Informationen zu diesem Dokument

Dokumentenklasse:	öffentlich
Dokumententitel:	Bericht zur Informationssicherheit 2 Halbjahr / 2019
Verantwortliche/r Autor/in:	Merlin Wolf
Dateiname:	2020-01-20_Bericht_2H_2019
Fassung vom:	20.01.2020
Letzte Veröffentlichung:	20.01.2020
Seitenzahl:	11
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

1. Gefährdungslage 2. Halbjahr / 2019 6

1.1 Mail Security 6

1.1.1 Gefilterte Mails 6

1.1.2 Zusammensetzung der schadhaften Mails 8

1.2 Endpoint Security 10

2. Emotet Angriff auf die städtischen IT-Systeme 11

Abbildungsverzeichnis

Mail Security

Abbildung 1Verteilung von Echten-Mails und Junk-Mails.....6
Abbildung 2 Verteilung von Echten-Mails und Junk-Mails pro Monat in Q3 / 2019 .7
Abbildung 3 Verteilung von Echten-Mails und Junk-Mails pro Monat in Q4 / 2019 .7
Abbildung 4 Zusammensetzung Junk-Mails im 2. Halbjahrs 2019 8
Abbildung 5 Verlauf Viren und Phishing Q3 / 2019 8
Abbildung 6 Verlauf Viren und Phishing Q2 / 2019 9
Abbildung 7 Verlauf von Viren und Phishing ab Q1 / 2019.....9

Endpoint Security

Abbildung 8 Anteil von Malware und IPS Ereignissen im 2. Halbjahr / 2019.....10
Abbildung 9 Verlauf Malware und IPS Ereignisse ab Q1 / 2019 10

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. Gefährdungslage 2. Halbjahr / 2019

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

1.1 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.

1.1.1 Gefilterte Mails

Im 2. Halbjahr 2019 sind bei der Stadtverwaltung Koblenz insgesamt 1.356.481 vom Provider KEVAG-Telekom bereits sicherheitstechnisch vorgefilterte E-Mails von externen Absendern eingegangen. Von diesen E-Mails wurden durch die städtischen Sicherheitssysteme noch einmal 770.431 E-Mails herausgefiltert. Der Anteil der sog. „Junk-Mails“, die eine potenzielle Bedrohung für die Systeme der Stadtverwaltung Koblenz darstellten, betrug hiernach 56,80%.

	Zusammensetzung Junk-Mails 2. Halbjahr 2019		
	Mails	Echt	Junk
gesamt	1.356.481	586.050 (43,20 %)	770.431 (56,80 %)

Abbildung 1Verteilung von Echten-Mails und Junk-Mails

Betrachtet man die Verteilung von „echten Mails“ und „Junk-Mails“ im 2. Halbjahr 2019 so kann man feststellen, dass die Anzahl an zugestellten Junk-Mails weiterhin zunahm.

	Zusammensetzung Junk-Mails Q3 / 2019		
	Mails	Echt	Junk
Juli	224.537	83.754 (37,30 %)	140.783 (62,70 %)
August	202.689	104.033 (51,33 %)	98.656 (48,67 %)
September	203.696	94.022 (46,16 %)	109.674 (53,84 %)
gesamt	630.922	281.809 (44,67 %)	349.113 (55,33 %)

Abbildung 2 Verteilung von Echten-Mails und Junk-Mails pro Monat in Q3 / 2019

	Zusammensetzung Junk-Mails Q4 / 2019		
	Mails	Echt	Junk
Oktober	235.589	102.914 (43,68 %)	132.675 (56,32 %)
November	238.202	107.209 (45,01 %)	130.993 (54,99 %)
Dezember	251.768	94.118 (37,38 %)	157.650 (62,62 %)
gesamt	725.559	304.241 (41,93 %)	421.318 (58,07 %)

Abbildung 3 Verteilung von Echten-Mails und Junk-Mails pro Monat in Q4 / 2019

1.1.2 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
- CM
- DHA
- Phishing
- Richtlinienverletzungen

Betrachtet man die Zusammensetzung der „Junk-Mails“ in den einzelnen Monaten des 2. Halbjahrs 2019 so fällt auf, dass die Anzahl der eingehenden Phishing Mails leichten Schwankungen unterlag – tendenziell jedoch niedrig bleibt; die Zahl der E-Mails mit schädlichen Viren hingegen in der zweiten Hälfte des zweiten Halbjahres sogar deutlich zugenommen hat und weiterhin auf einem hohen Niveau geblieben ist. Das Gefahrenpotenzial für die Systeme und Daten der Stadtverwaltung Koblenz bleibt daher nach wie vor unverändert hoch.

	Zusammensetzung Junk-Mails 2019						
	Junk	Spam	Virus	Phishing	Richtlinienverletzung	DHA	CM
2. Halbjahr	770.431	147.832 (19,19 %)	820 (0,11 %)	290 (0,04 %)	22.769 (2,96 %)	70.852 (9,20 %)	527.868 (68,52 %)

Abbildung 4 Zusammensetzung Junk-Mails im 2. Halbjahrs 2019

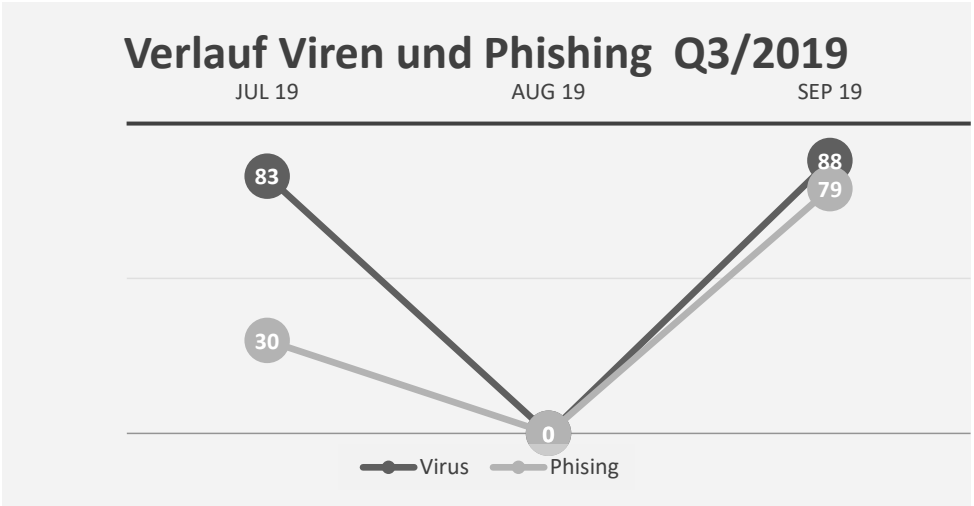

Abbildung 5 Verlauf Viren und Phishing Q3 / 2019

Hinweis: *Für den Monat August 2019 wurden dem Informationssicherheits- und Datenschutzmanagement keine Daten mitgeteilt.*

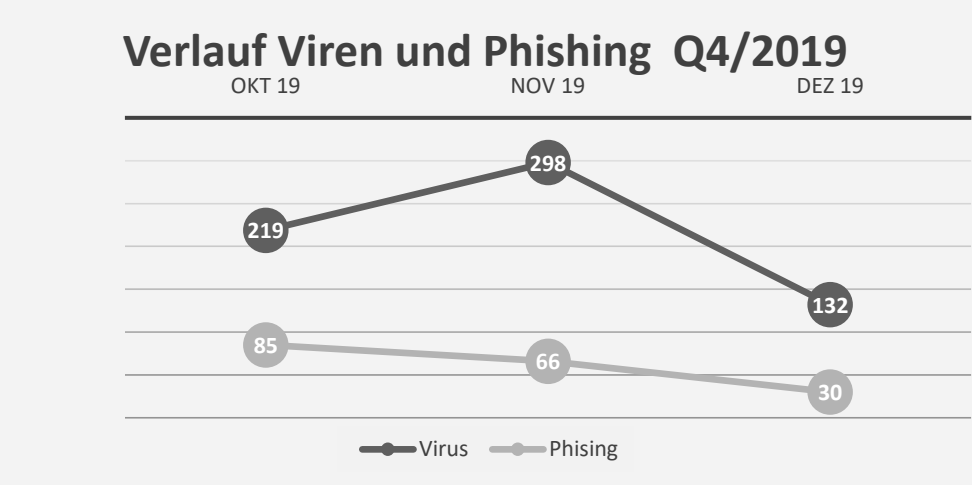

Abbildung 6 Verlauf Viren und Phishing Q2 / 2019

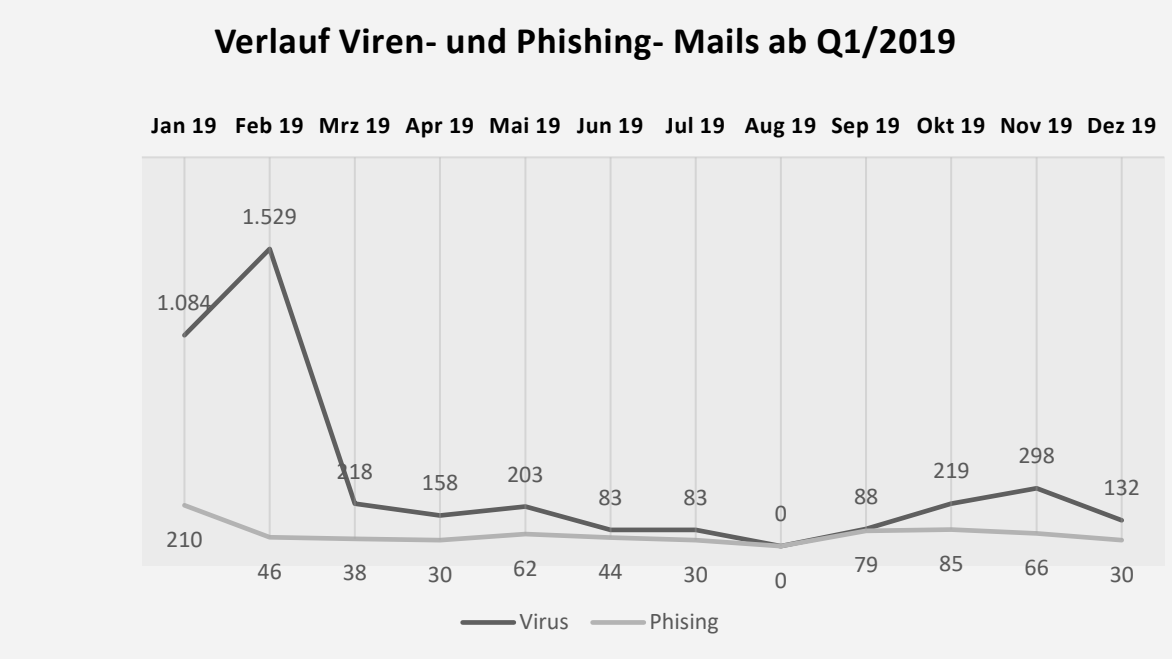

Abbildung 7 Verlauf von Viren und Phishing ab Q1 / 2019

1.2 Endpoint Security

Das Kommunale Gebietsrechenzentrum Koblenz setzt zur Absicherung der Endgeräte wie z. B. Computer, Notebooks etc. mehrere Systeme ein, unter anderem eine IPS (Intrusion Prevention System) und eine Endpoint-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 2. Halbjahrs 2019.

	Zusammensetzung Endpoint			
	Endpoint	Malware	ATD	IPS
2. Halbjahr	1.260	273 (21,67 %)	1 (0,08 %)	986 (78,25 %)

Abbildung 8 Anteil von Malware und IPS Ereignissen im 2. Halbjahr / 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 21,67% erneut durch den lokalen Virenscanner abgewehrt werden.

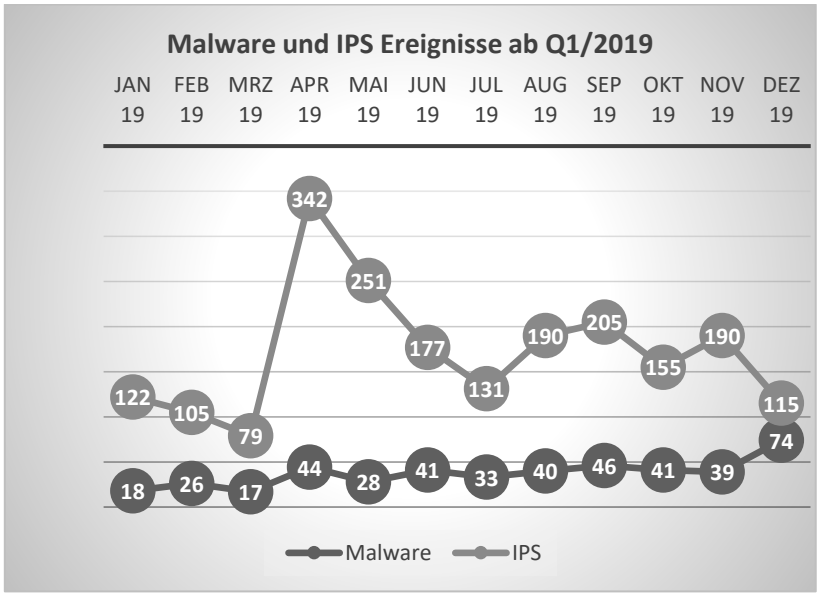

Abbildung 9 Verlauf Malware und IPS Ereignisse ab Q1 / 2019

2. Emotet Angriff auf die städtischen IT-Systeme

Bereits am 17.12.2019 lagen dem KGRZ erste Anzeichen für aktuelle Spamwelle vor. Die Gesamtverwaltung wurde daraufhin durch das KGRZ per Mail informiert und um erhöhte Aufmerksamkeit bei eingehenden Mails gebeten.
Am Morgen des 18.12.2019 bemerkten die Kollegen des Teams für E-Collaboration des KGRZ im Rahmen des mobil-device-Managements eine Auffälligkeit bei der Mail-Adresse strassenbeleuchtung@stadt.koblenz.de. Im Verlauf des Morgens wurde das Security Management durch einen Bürger per E-Mail darüber informiert, dass er am 14.11.2019 eine E-Mail an die Adresse strassenbeleuchtung@stadt.koblenz.de gesendet habe, in der er einen Hinweis zu einer defekten Straßenbeleuchtung gegeben habe.
Nun habe er am 18.12.2019 mehrere Antworten auf seine damalige E-Mail erhalten, alle mit dem gleichen Anzeigename „strassenbeleuchtung“, allerdings von fünf verschieden E-Mail-Adressen.
Daraufhin wurde das Team E-Collaboration des KGRZ mit der Bitte um weitere Prüfung über die E-Mail des Bürgers informiert. Aufgrund der bereit vorliegenden Informationen war es dem Kommunalen Gebietsrechenzentrum innerhalb kürzester Zeit möglich, die Vorkommnisse einzuordnen und schließlich eine durch einen „Emotet“-Angriff infizierte Maschine beim Kommunalen Servicebetrieb Koblenz (EB70) zu identifizieren und sofortige Gegenmaßnahmen zu ergreifen.
Als Sofortmaßnahme wurde der betroffene Rechner aus dem Netzwerk der Verwaltung entfernt. Da es sich bei dem betroffenen System um eine virtuelle Maschine mit dem Betriebssystem Windows 7 handelte, wurden umgehend alle in der Verwaltung noch im Einsatz befindlichen Windows 7 Maschinen heruntergefahren und aus der Domäne entfernt. Durch diese Maßnahme konnte eine weitere Kompromittierung des Netzwerkes verhindert werden. Gleichzeitig wurden alle administrativen Accounts im Netzwerk gesperrt und für alle Rechner der Verwaltung der Internetzugang deaktiviert, um einen möglichen Datenabfluss zu verhindern.
Im Anschluss hieran wurden alle weiteren IT-Systeme mittels eines durch den Hersteller McAfee aktualisierten Viren-Pattern auf eine mögliche Kompromittierung gescannt. Glücklicherweise konnte hierbei keine weitere Kompromittierung festgestellt werden. Im weiteren Verlauf wurden alle Windows 7 Maschinen durch das KGRZ gegen Maschinen mit dem Betriebssystem Windows 10 ausgetauscht.