Landeshauptstadt
München
IT-Referat

Landeshauptstadt München, Referat für Informations- und Telekommunikationstechnik, 80335 München

Thomas Bönig
Berufsmäßiger Stadtrat

FDP Stadtratsfraktion
Herrn StR Dr. Matter
Frau StRin Neff
Herrn StR Prof. Dr. Hoffmann
Herrn StR Ranft
Herrn StR Zeilnhofer

Rathaus

Datum:
01.04.2020

Angriffe auf die Infrastruktur der Stadt durch Emotet?

Schriftliche Anfrage gemäß § 68 GeschO
Anfrage Nr. 14-20 / F 01751 von Herrn StR Dr. Michael Matter, Frau StRin Gabriele Neff, Herrn StR Thomas Ranft, Herrn StR Prof. Dr. Jörg Hoffmann, Herrn StR Wolfgang Zeilnhofer vom 11.03.2020, eingegangen am 11.03.2020

Sehr geehrte Damen und Herren,

in Ihrer Anfrage haben Sie folgenden Sachverhalt vorausgeschickt:

„Seit einiger Zeit treibt die Schadsoftware Emotet im Internet ihr Unwesen. Dabei wird sie besonders trickreich in E-Mails getarnt, die so gestaltet sind, dass den meisten Empfängern nicht auffällt, dass es sich um einen Betrug handelt. Die E-Mails kommen von Absendern des eigenen Adressbuches oder von Leuten mit denen man bereits in Kontakt stand. Öffnet man den Anhang der E-Mail lädt die Schadsoftware weitere Programme unbemerkt nach. Bei unkontrolliertem Befall eines Systems wird das komplette System gekapert und eine Lösegeldsumme für die Freigabe verlangt. Besonders für große Netzwerke wie beispielsweise das der Landeshauptstadt München (LHM) birgt der Schädling enorme Gefahren.

Zu den im Einzelnen gestellten Fragen kann ich Ihnen Folgendes mitteilen:

Frage 1
Gab es Angriffe bzw. Schädigungen durch Emotet auf die Infrastruktur der LHM?

Agnes-Pockels-Bogen 21
80992 München
Telefon: 089 233 – 767777

Antwort
Die Entstehungsgeschichte der Schadsoftware Emotet geht zurück bis in das Jahr 2014, in dem sie das erste Mal durch einen Hersteller von Antiviren-Software identifiziert wurde. Seitdem hat Emotet eine vielfältige Entwicklung vollzogen, die sich in immer umfangreicheren Funktionen zur Kompromittierung von IT-Systemen niedergeschlagen hat. Die aktuelle Evolutionsstufe wurde grob gesagt im Laufe des Jahres 2019 erreicht und hat zu vielfältigen Schäden in den IT-Infrastrukturen weltweit geführt.

Auch die Landeshauptstadt München war im Jahr 2019 von Emotet betroffen.

In diesem Zusammenhang ist wichtig zu wissen, dass die Infektion eines IT-Systems mit Emotet in verschiedenen Stufen erfolgt. Im Rahmen des Security-Incident-Managements der LHM werden diesbezüglich drei Stufen unterschieden. In Stufe 1 geht es um die Ausführung oder den Versuch der Ausführung von initialem Emotet-Schadcode. Stufe 2 umfasst spezifische Aktivitäten von Emotet, etwa dem Nachladen von zusätzlichem Schadcode oder der Weiterverbreitung im lokalen Netzwerk. Stufe 3 bezieht sich schließlich auf das Auftreten von konkreten Schadwirkungen durch Emotet, wie z. B. der Verschlüsselung von Daten.

Bei allen durch das Informationssicherheitsmanagement in der LHM registrierten Vorfällen im Kontext Emotet im Jahr 2019 konnte durch die jeweilige Vorfallsbehandlung (Incident Reponse) ein Auftreten von Schadwirkungen in Stufe 3 unterbunden werden. Vorfälle in Stufe 1 wurden im Jahr 2019 im mittleren zweistelligen Bereich auf IT-Systemen der LHM detektiert. In vereinzelten Fällen konnten darüber hinaus Aktivitäten in Stufe 2 erkannt werden.

Alle diese Vorfälle konnten durch die definierten Maßnahmen zur Vorfallsbehandlung im Rahmen des Informationssicherheitsmanagements rechtzeitig adressiert werden. Betroffene IT-Systeme wurden in diesem Zusammenhang umgehend vom Verwaltungsnetz getrennt und entsprechende Bereinigungsmaßnahmen wurden eingeleitet. In einem Fall eines Stufe 2-Vorfalls wurden zudem zwei Netzsegmente vorbeugend vom Verwaltungsnetz entkoppelt, um eine potentielle Weiterverbreitung von Emotet im Verwaltungsnetz zu unterbinden.

Neben diesen konkreten Vorfällen auf IT-Systemen der LHM ist die Erkennung von Schadsoftware am Perimeter unserer IT-Infrastruktur ein weiterer Indikator für die Betroffenheit der LHM durch Emotet. In diesem Kontext wurden insbesondere an unseren E-Mail-Servern im Jahr 2019 eine hohe Anzahl von mehreren tausend E-Mails als potentiell mit Emotet infiziert erkannt und abgefangen, bevor sie auf Endgeräte der LHM gelangen konnten.

Zusammenfassend kann festgehalten werden, dass die LHM im Jahr 2019 in einem für Organisationen vergleichbarer Größe wohl üblichem Maß mit Emotet konfrontiert war. Größere Schäden, mit Ausnahme von zeitweiligen Einschränkungen im Hinblick auf die Verfügbarkeit von bestimmten IT-Systemen, konnten jedoch vermieden werden.

Frage 2
Wie wurden die Mitarbeiter vor den Angriffen gewarnt oder vorbereitet?

Antwort
Im Rahmen des Informationssicherheitsmanagements der LHM werden sogenannte Awareness-Maßnahmen definiert und umgesetzt, durch die Mitarbeiter*innen für Aspekte der Informationssicherheit im Rahmen der täglichen Arbeit sensibilisiert werden.

Aufbauend auf diesen grundsätzlichen Maßnahmen wurden Mitarbeiter*innen speziell im Hinblick auf mögliche Gefährdungen durch Emotet und relevante Verhaltensweisen sensibilisiert. Dies erfolgte durch direkte E-Mailkommunikation in der Organisation sowie durch entsprechende Publikationen im Intranet der LHM.

Diese Aktivitäten werden in der Regel im Einklang mit entsprechenden Warnmeldungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder des Landesamtes für Sicherheit in der Informationstechnik (LSI) durch das stadtweite Informationssicherheitsmanagements im IT-Referat initiiert und dezentral durch die Informationssicherheitsbeauftragten der Referate und Eigenbetriebe für den jeweiligen Verantwortungsbereich angepasst und propagiert.

Für die Beschäftigten in der IT beim IT-Referat und bei it@M stehen jenseits der allgemeinen Sensibilisierung für Emotet natürlich dessen technische Aspekte im Vordergrund. Ein Schwerpunkt dabei liegt auf der Konzeption und Umsetzung von relevanten IT-Sicherheitsmaßnahmen, um eine Infektion möglichst frühzeitig auf Netzwerk- oder Systemebene erkennen zu können. In diesem Zusammenhang wurden z. B. die Filterregeln für eingehende E-Mails auf Emotet-typische Muster angepasst oder auch die Möglichkeiten zur Erkennung von verdächtiger Netzwerkkommunikation deutlich angehoben.

Im Rahmen des Informationssicherheitsmanagements ist gerade der letztgenannte Aspekt auch zukünftig von zentraler Bedeutung für eine wirksame Erkennung und Abwehr von Schadsoftware auf IT-Systemen der LHM sowie im Verwaltungsnetz. Aktuell wird dieser Bereich im Cyber Security Center bei it@M aufgebaut und muss auch in den folgenden Jahren kontinuierlich entwickelt werden.

Frage 3
Wie sieht die LHM die Gefahr auf Grund von Computerschadcodes nach der Umstellung von Linux zurück auf Windows?

Antwort
Aus dem Blickwinkel des Informationssicherheitsmanagements ist das Betriebssystem ein wichtiger Faktor, wenn es um den Schutz der verarbeiteten Informationen geht. In diesem Zusammenhang sind jedoch nicht nur grundlegende Systemarchitekturen oder technische Sicherheitsfunktionen zu betrachten bzw. zu vergleichen, um das Gefährdungspotential für ein bestimmtes Betriebssystem zu beurteilen. Relevant sind auch weiterführende Aspekte, wie

zum Beispiel der Verbreitungsgrad eines Betriebssystems, die dazu beitragen können, dass ein bestimmtes Betriebssystem besonders attraktiv für Entwickler von Schadsoftware ist.

Im Hinblick auf den letztgenannten Aspekt ist etwa festzuhalten, dass Windows 10 im Februar 2020 einen geschätzten weltweiten Marktanteil von ca. 57 % bei Client-Systemen aufweist, die gesamte Windows-Familie sogar knapp 88 % (Quelle: NetMarketShare - https://netmarketshare.com/operating-system-market-share.aspx).

Dieser hohe Verbreitungsgrad trägt natürlich dazu bei, dass Windows als Betriebssystem deutlich klarer im Fokus von Schadsoftware und deren Entwicklern steht als beispielsweise Linux. Dieser Effekt wird zusätzlich verstärkt, da sich im Laufe der Zeit sehr vielfältige kriminelle Geschäftsmodelle im Bereich Malware entwickelt haben, die, wie im Fall von Emotet, zum Beispiel auch auf die Erpressung von Opfern hinauslaufen. Je höher die Anzahl möglicher Zielsysteme also ist, um so attraktiver ist das jeweilige Segment für die Cyber-Kriminellen, die hinter solchen Schadprogrammen stehen. Auf der anderen Seite be- und entsteht hierdurch natürlich ein sehr großer Markt für spezialisierte Hersteller und Dienstleister im IT-Sicherheitsumfeld von Windows. Die LHM als Kunde solcher Lösungen kann in diesem Bereich daher auf ein deutlich größeres Angebots- und Leistungsspektrum zurückgreifen als dies beispielsweise in Bezug auf Linux der Fall ist.

Vor diesem Hintergrund geht aus Sicht des Informationssicherheitsmanagements der LHM mit der Umstellung von Linux auf Windows eine grundsätzlich gesteigerte Gefährdungslage einher. Diese Beurteilung ist lediglich auf Grundlage des hohen Verbreitungsgrades von Windows zu interpretieren und trifft keine Aussage darüber, ob nun Windows oder Linux aus technologischen Gesichtspunkten das sicherere Betriebssystem darstellt.

Für die LHM bedeutet diese Einschätzung, dass die Maßnahmen zur Aufrechterhaltung der Informationssicherheit intensiviert werden müssen. Dies gilt jedoch nicht nur im Hinblick auf die Absicherung der Endgeräte unter Windows, sondern z. B. auch für die Serversysteme oder das Verwaltungsnetz. Denn das Beispiel Emotet zeigt sehr eindringlich, dass nur ineinandergreifende IT-Sicherheitsfunktionen in unterschiedlichen Bereichen unserer IT-Infrastruktur es ermöglichen, solche Gefährdungen wirksam abzuwehren. Es ist somit nicht getan mit einer alleinigen Installation von Malware-Schutzprogrammen auf Endgeräten. Die LHM muss in integrierte IT-Sicherheitssysteme investieren, die Bedrohungen z. B. anhand von Anomalien im Netzwerkverkehr erkennen, ihre Kritikalität bestimmen und automatisiert Gegenmaßnahmen einleiten. Nur durch einen derartigen Ausbau der IT-Sicherheitsarchitektur der LHM kann der stetig steigenden Bedrohungslage durch Cyberkriminalität wirkungsvoll begegnet werden.

Abschließend möchten wir darauf aufmerksam machen, dass die im Rahmen der Beantwortung dargestellten Zusammenhänge nicht ausschließlich im Kontext von Emotet oder der Diskussion über Betriebssysteme Gültigkeit aufweisen. Vielmehr haben sie grundlegenden Charakter. Denn nur wenn unsere Informationen sicher verarbeitet und übertragen werden, können wir bei der LHM verlässliche digitale Services für unsere Bürger*innen, Unternehmen und Partner anbieten.

Informationssicherheit stellt somit eine der wesentlichen Voraussetzungen für eine erfolgreiche Digitalisierung der Landeshauptstadt München dar. Sie muss jedoch mit der hohen Dynamik in diesem Bereich und der Vielzahl an neuen IT-Services Schritt halten können. Hierfür ist es unerlässlich, dass gezielt in die Informationssicherheit und deren Entwicklung investiert wird.

Mit freundlichen Grüßen

gez.
Thomas Bönig
IT-Referent