M. Meier, D. Reinhardt, S. Wendzel (Hrsg.): Sicherheit 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 171

Practitioners Track: Lessons learned bei KMUs aus dem Befall durch Ransomware

Florian Hertle[1]

Abstract: Am Beispiel eines konkreten Projekts wird gezeigt, welche aktuelle Gefährdungslage für KMUs aus grassierender Ransomware besteht. Mit Hilfe eines halb-automatisierten Vorgehens wurde bei einem KMU die IT-Landschaft, mit ca. 350 Clients und ca. 120 Servern, auf mit Ransomware infizierte Systeme geprüft. Per Anmeldeskript wurden von den Systemen verschiedene „Cryptowall 3.0"-spezifische Indikatoren gesammelt und anschließend per Skript aufbereitet. Auffälligkeiten wurden an den Systemen manuell überprüft. Zur Prävention vor neuen Malwareinfizierungen wurden Maßnahmen zur Erreichung eines Mindestniveaus der Informationssicherheit erarbeitet. Auf Basis eines Quick-Checks der vorhandenen technischen und organisatorischen Maßnahmen, wurde, per Bottom-Up Ansatz, entsprechende Quick-Wins abgeleitet.

Keywords: IT-Forensik, Verteidigungstechniken, Malware, Ransomware, Cryptowall 3.0, Mindestniveau, KMU, it.sec

1 Einleitung

Die Bedrohung durch Schadsoftware, die Dateien verschlüsselt und anschließend ein Lösegeld fordert (sogenannte Ransomware), hat sich im Jahr 2014 im Vergleich zum Jahr 2013 auf das 45-Fache erhöht [Wo15]. Auch im Jahr 2015 waren eine Vielzahl von Unternehmen von Cryptowall, Cryptolocker, Chimera und Co. betroffen. Ransomware beschränkt sich dabei nicht nur auf das Verschlüsseln lokaler Dateien, es werden auch Dateien auf Netzlaufwerken verschlüsselt, sofern der Benutzer darauf Zugriff hat. In der Regel beträgt das Lösegeld meist zwischen 300 und 1.000 EUR. Dieses Lösegeld ist mittels Bitcoins zu bezahlen.

Ransomware wird über verschiedenste Wege verbreitet. Der Hauptverbreitungsweg stellen E-Mails mit schadhaften Anhängen dar [Wo15]. Dabei kommen hauptsächlich ausführbare Dateien (.exe), JavaScript-Dateien (.js) und Word-Dokumente mit Makros (.doc, .docm) zum Einsatz. Die Polizei in Niedersachsen warnte am 12. Oktober 2015 von einer Ransomware namens „Chimera", die sich über fingierte Bewerbungen verbreitet hat. Die als Bewerbungsunterlagen getarnte Schadsoftware wurde dabei per Dropbox Link zur Verfügung gestellt [Po15]. Weitere Infektionswege stellen der Download von infizierten Dateien aus dem Internet und der Aufruf von

[1] it.sec GmbH & Co. KG, Einsteinstraße 55, 89077 Ulm, fhertle@it-sec.de

kompromittierten Webseiten dar. Seit Ende 2015 wird Ransomware vermehrt auch über Exploit Kits (Tool zur automatisierten Ausnutzung verschiedener Softwareschwachstellen) verteilt [Th15].

2 Aufgabenstellung

Bei einem KMU (kleine und mittlere Unternehmen) wurden drei Systeme im Zeitraum von wenigen Monaten mit der Ransomware „Cryptowall 3.0“ infiziert und sowohl lokale Dateien, als auch Netzlaufwerke verschlüsselt. Betroffen waren ein Geschäftsführer, der Leiter Vertrieb und ein Vertriebsmitarbeiter. In zwei der drei Fälle konnten die verschlüsselten Daten durch interne Sicherungsmaßnahmen größtenteils zurückgespielt werden. Im dritten Fall musste das Lösegeld bezahlt werden, um die Daten wiederherzustellen.

Aufgrund des Netzwerkdesigns wurde die Schadsoftware erst aktiv, als sich die Systeme mit einem externen Netzwerk (z.B. WLAN Hotspot) verbunden haben. Im internen Netzwerk wird der Port 80 an der Firewall geblockt, da die Internetverbindung nur über einen Proxyserver möglich ist. Somit bestand das Risiko, dass auf weiteren Systemen eine Malwareinfektion vorliegt/schlummert, ohne dass diese Kontakt mit dem C&C Server (Command & Control) aufnehmen konnte. Daraufhin wurde die it.sec beauftragt, die Frage zu beantworten, ob weitere Systeme mit der Ransomware „Cryptowall 3.0“ infiziert sind.

2.1 Informationen zum Unternehmen

Das Produktionsunternehmen ist in den letzten Jahren stark gewachsen, ohne dass die IT-Abteilung in gleichem Maße mit gewachsen ist. Derzeit betreuen fünf IT-Mitarbeiter eine sehr heterogene Systemlandschaft (ca. 120 Server und ca. 350 Clients) in mehreren Ländern. Als Betriebssystem kommen fast alle Versionen zwischen Windows 2000 Server bis Windows 7 zum Einsatz. Eine Standardisierung der Clients war bisher nicht möglich, da eine Vielzahl der Benutzer lokale Administratorberechtigungen für die Nutzung des ERP-Systems benötigen. Regelungen zum Umgang mit IT-Equipment waren nur rudimentär vorhanden.

3 Lösungsstrategie / Projektablauf

Die Fragestellung des Projekts lautete: „Sind weitere Systeme mit „Cryptowall 3.0“ infiziert?“. Aufgrund der Tatsache, dass aktuelle Malware nicht oder nicht sehr zuverlässig von Virenscannern erkannt wird, kann diese Frage nicht einfach durch einen Virenscan aller Computer beantwortet werden. Beispielsweise wurden durch die Cyber Threat Alliance im Zeitraum vom 01. August 2015 bis zum 31. Oktober 2015 1924

unterschiedliche „Cryptowall 3.0“ Varianten registriert, so dass für jede einzelne Variante ein spezielles Pattern des Virenscanners vorhanden sein müsste, um diese zuverlässig zu erkennen [Ct16]. Des Weiteren stellt eine manuelle Analyse aller Systeme eine nicht wirtschaftliche Lösung dar, weshalb es notwendig war ein Vorgehen zu entwickeln, um die Anzahl der manuell zu überprüfenden Systeme zu reduzieren. Hierzu wurde ein zwei-stufiges Vorgehen gewählt. In der ersten Stufe wurde ein Quick-Check der Informationssicherheit (Bestandsaufnahme der vorhandenen technischen und organisatorischen Maßnahmen) und eine Log-File Analyse der Firewall und des Virenscanners durchgeführt. Aufbauend auf die Ergebnisse der 1. Stufe wurde in der zweiten Stufe die Prüfung auf Malwareinfizierung durchgeführt. Hierzu wurde ein Skript entwickelt, um Indikatoren für eine „Cryptowall 3.0“ Infizierung zu sammeln, so dass auffällige Systeme identifiziert werden können, um diese manuell zu überprüfen.

Ausgehend von verschiedenen Malwareanalysen von „Cryptowall 3.0“-Binaries wurden folgende Indikatoren abgeprüft:

- Registry Einträge für Autostart
- Status und Einstellungen zu Volume Shadow Copy Service (VSS), da dies durch die Malware gestoppt wird
- Status zu verschiedenen Diensten (Sicherheitscenter, Windows Update, …), da diese ebenfalls durch die Malware gestoppt werden
- Windows Startkonfiguration
- Liste der Prozesse
- Liste der Dienste

Aufgrund der heterogenen Systemlandschaft sollten dabei hauptsächlich Windows eigene Tools zum Einsatz kommen, die in möglichst allen Betriebssystemversionen vorhanden sind, so dass hauptsächlich die Kommandozeilenbefehle „wmic“, „vssadmin“, „sc“ und „reg“ genutzt wurden. Das Batch-Skript konnte bei den meisten Systemen per Windows Gruppenrichtlinie als Anmeldeskript hinterlegt werden. Nach Ablauf einer gewissen Zeit wurden die gesammelten Indikatoren per Python Skript aufbereitet und die Auffälligkeiten (z.B. Autostart Eintrag in Appdata-Verzeichnis) ausgewertet. Dabei konnte ein System identifiziert werden, auf dem ein Malware Dropper (kompromittiert das System und lädt eigentlichen Schadcode nach) gefunden werden konnte. In der ersten Analyse wurden ca. 300 Systeme analysiert. Die Analyse wurde nach Ablauf einer weiteren Frist erneut durchgeführt, um die restlichen Systeme zu prüfen.

Im Rahmen der Log-File Analyse wurden bereits einzelne Systeme als auffällig identifiziert (geblockter Zugriff über Port 80 (http) und 443 (https) auf dubiose IP-Adresse). Da der Wissenstransfer zum Kunden elementarer Bestandteil des Projekts war, wurden die ersten Untersuchungen der auffälligen Systeme gemeinsam durchgeführt. Weitere Systeme konnten anschließend durch den Kunden selbst analysiert werden.

Im Rahmen des Lessons Learned Prozesses wurden Maßnahmen abgeleitet, um ein Informationssicherheitsmindestniveau zu erreichen. Hierzu wurde das Ergebnis des Quick-Checks mit der Risikosituation des Unternehmens abgeglichen. Per Bottom-Up Ansatz wurden Maßnahmen ausgewählt, die zur schnellen Verbesserung der Informationssicherheit beitragen.

4 Herausforderungen bei der operativen Durchführung

Durch die Entscheidung für einen halb-automatisierten Ansatz haben sich verschiedene Herausforderungen ergeben. Das Skript zum Sammeln der Indikatoren wurde von ca. 10% der Benutzer abgebrochen, so dass die Indikatoren nicht von allen Systemen vollständig vorlagen. Dies war möglich, da das Anmeldeskript nicht im Hintergrund ausgeführt wird. Um im Auswerteskript Fehler aufgrund von fehlenden Indikatoren zu vermeiden, wurde ein zusätzliches Prüfskript erstellt, welches eine Liste der Systeme mit vollständigen Indikatoren erstellt. Diese Liste wurde als Basis für das Skript zum Aufbereiten der Indikatoren verwendet.

Um sicherstellen zu können, dass alle Systeme analysiert wurden, ist eine Liste aller Systeme notwendig. Diese war jedoch nicht standardmäßig im Unternehmen vorhanden. Mit Hilfe der Softwareverteilungssoftware konnte eine Behelfsliste nachträglich erzeugt werden.

Die heterogene Systemlandschaft konnte auf Systeme mit mindestens Windows XP reduziert werden, so dass lediglich zwei unterschiedliche Skripte erstellt werden mussten: Ein Skript für Windows XP und Windows 2003 Server Systeme und ein zweites Skript für Versionen Windows 7 und die entsprechende Server Systeme.

Die älteren Systeme (ca. 5) wurden gegen Ende des Projekts manuell durch den Kunden überprüft.

Wie bereits erwähnt, arbeitet die Vielzahl der Benutzer mit lokalen Administratorberechtigungen. Diese werden von den Mitarbeitern genutzt, um beliebige Software zu installieren. Dies führt zu einem dazu, dass es nicht zielführend ist, die Systeme gegen ein „Baseline System“ abzugleichen und zum anderen hat es zu mehreren False-Positives geführt, da sogenannte PUPs (potentiell unerwünschte Programme) installiert waren.

Beim Auswerten der Indikatoren wurden die verschiedenen Indikatoren in einzelnen Text-Dateien (%COMPUTERNAME%-INDIKATOR-XX.txt) gespeichert. Teilweise waren diese bei unterschiedlichen Systemen unterschiedlich kodiert. Deshalb musste die Kodierung entsprechend in den Skripten hinterlegt und angepasst werden.

5 Fazit

Die Implementierung eines Virenscanners stellt keinen ausreichenden Schutz vor Schadsoftware dar. Weder die Ransomware, noch der Dropper wurde vom Virenscanner erkannt. Eine ganzheitliche Betrachtung der Informationssicherheit findet leider nur bei wenigen KMUs statt. Die derzeit akute Bedrohungslage durch Ransomware für KMUs sollte als Ausgangspunkt verwendet werden, die Informationssicherheit des eigenen Unternehmens zu überprüfen. Im vorgestellten Projekt wurde dies erst nach mehreren Vorfällen als notwendig erachtet. Deshalb beschränkte sich das Projekt nicht nur auf die Erkennung von weiteren Malwareinfizierungen, sondern der Kunde wurde auch bei der Verbesserung von präventiven Maßnahmen unterstützt und begleitet (z.B. Einführung einer ordnungsgemäßen Passwortpolicy und Vermeidung von lokalen Administratorberechtigungen). Der gewählte Bottom-Up Ansatz hilft, hier schnell Ergebnisse zu liefern, jedoch sollte langfristig auf einen Top-Down Ansatzes (beispielsweise in Anlehnung an die ISO/IEC 27001:2013) umgestellt werden. Auch ohne akuten Malwarevorfall sollte jedes Unternehmen überprüfen, ob alle Basisschutzmaßnahmen entsprechend implementiert sind und alle notwendigen Unternehmensbereiche abdecken.

Ergänzend zu den technischen und organisatorischen Maßnahmen muss die Awareness der Mitarbeiter zwingend verbessert werden. In den letzten Jahren hat die Qualität von SPAM und Phishing E-Mails zugenommen, so dass auch die Mitarbeiter besser auf die neuen Gefahren vorbereitet werden müssen. Einfache Qualitätskriterien, wie z.B. Rechtschreibung, Grammatik, Sprache, reichen zunehmend nicht mehr aus, solche E-Mails von regulären E-Mails zu unterscheiden. Vielmehr muss eine inhaltliche Prüfung der E-Mail auf Konsistenz (z.B. erwarte ich von einer Bewerbung eines Dachdeckers die Vorlage von verschiedenen Zertifikaten) und eine Prüfung der Dateiendungen der E-Mail Anhänge stattfinden.

Generell gilt, dass das Bezahlen der Lösegeldforderung vermieden werden sollte, um den Anreiz bei Angreifern nicht weiter zu erhöhen.

Literaturverzeichnis

[Ct16] Cyber Threat Alliance, http://cyberthreatalliance.org/cryptowall-dashboard.html, Stand: 27.01.2016.

[Po15] Polizei Niedersachsen, http://www.polizei-praevention.de/aktuelles/chimera-ransomware.html, Stand: 16.12.2015.

[Th15] Threatpost, Kaspersky Lab, https://threatpost.com/angler-exploit-kit-spreading-cryptowall-4-0-ransomware/115538/, Stand: 16.12.2015.

[Wo15] Wood, P.: Symantec Internet Security Threat Report, Volume 20, Mountain View, CA: Symantec Corp, 2015.