Bundesamt
für Sicherheit in der
Informationstechnik

Lagedossier Ransomware

Stand Mai 2016

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Internet: https://www.bsi.bund.de
© Bundesamt für Sicherheit in der Informationstechnik 2016

Inhaltsverzeichnis

1 Zusammenfassung ... 5

2 Ransomware ... 6

2.1 Historie ... 6

2.2 Funktionsweise ... 6

2.2.1 Ransomware mit Sperrbildschirmen ... 6

2.2.2 Ransomware mit Verschlüsselung ... 7

2.2.3 Weitere Eigenschaften ... 8

2.2.4 Lösegeldzahlung ... 9

2.3 Plattformen ... 10

2.4 Verschlüsselung ... 13

3 Bedrohungslage ... 15

3.1 Angriffsvektoren ... 16

3.1.1 Angriffsvektor Spam ... 16

3.2 Angriffsvektor Drive-by-Angriffe mittels Exploit Kits ... 18

3.3 Angriffsvektor Schwachstellen in Server-Software ... 19

3.4 Nachladen von Ransomware bei bestehenden Schadsoftware-Infektionen ... 19

3.5 Angriffsvektoren manuelle bzw. gezielte Cyber-Angriffe mit Ransomware ... 20

3.6 Betroffenheit der deutschen Wirtschaft durch Ransomware ... 20

3.7 Schäden ... 21

3.7.1 Schäden für Privatpersonen ... 21

3.7.2 Schäden für Organisationen ... 21

3.8 Ausblick auf die Weiterentwicklung der Bedrohungslage ... 23

4 Maßnahmen ... 24

4.1 Präventionsmaßnahmen ... 24

4.1.1 Maßnahmen gegen den Angriffsvektor Spam ... 24

4.1.2 Maßnahmen gegen den Angriffsvektor Drive-by-Angriffe ... 25

4.1.3 Maßnahmen gegen weitere Angriffsvektoren ... 27

4.1.4 Datensicherungskonzept und Backup ... 27

4.1.5 Einsatz von Virenschutzprogrammen ... 28

4.1.6 Mitarbeitersensibilisierung und Awareness ... 28

4.1.7 Weitere Maßnahmen zum Schutz vor oder zur Reduktion der Auswirkungen nach einer Ransomware-Infektion ... 29

4.2 Detektionsmaßnahmen ... 32

4.2.1 Zentrale Sammlung und Auswertung von Logdaten ... 32

4.2.2 Zugriffe am Netzübergang auf Kontrollserver überwachen und ggf. blocken ... 32

4.3 Reaktionsmaßnahmen ... 33

4.3.1 Incident Response ... 33

4.3.2 Externe Expertise ... 34

4.3.3 Wiederherstellung der Daten ... 34

4.3.4 Lösegeld ... 35

4.3.5 Anzeige erstatten ... 35

5 Weitere Informationen ... 36

5.1 Pressemitteilungen und Kurzmeldungen des BSI sowie Beiträge der BSI-Mediathek zum Thema Ransomware ... 36

5.2 Allianz für Cyber-Sicherheit ... 36

Zusammenfassung

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes wieder freigeben. Cyber-Angriffe durch Ransomware sind eine Form digitaler Erpressung.

Ransomware, die den Zugang zu einem System sperrt oder unterbindet, verankert sich im infizierten System. Der Arbeitsplatz wird mit einem Bild oder einer Webseite überlagert, in der der Nutzer über die Sperrung des Systems informiert und zu einer Zahlung aufgefordert wird. Diese Form von Ransomware spielt auf Desktop-Systemen heute fast keine Rolle mehr.

Ransomware, die Daten verschlüsselt, nutzt oder kombiniert symmetrische und/oder asymmetrische Verfahren zur Verschlüsselung von Nutzerdaten. Bei korrekter Implementierung ist die Wiederherstellung der verschlüsselten Daten nur mit dem passenden Schlüssel möglich.

Viele Ransomware-Familien verschlüsseln neben lokalen Laufwerken auch angeschlossene externe Medien (z.B. USB-Sticks) sowie Netzlaufwerke und nutzen weitere Methoden, um die Wiederherstellung von Daten zu erschweren. Gerade in Unternehmensnetzen mit weitreichenden Zugriffsmöglichkeiten können dadurch einzelne, mit Ransomware infizierte Systeme unternehmensweite Datenverluste verursachen.

Die bekannten und weit verbreiteten Ransomware-Familien zielen fast ausschließlich auf das Betriebssystem Microsoft Windows. Darüber hinaus gibt es jedoch auch Ransomware-Familien, die auf das Desktop-Betriebssystem Apple MacOS X, Server-Systeme unter GNU/Linux und mobile Betriebssysteme wie Google Android abzielen. Die Verbreitung von Ransomware auf diesen Plattformen ist, im Vergleich zu Microsoft Windows, jedoch gering.

Die häufigsten Angriffsvektoren, über die Systeme mit Ransomware infiziert werden, sind Anhänge von Spam-E-Mails sowie Drive-by-Angriffe mittels Exploit-Kits.

Nach Auswertung der dem BSI vorliegenden Daten war Deutschland im ersten Quartal 2016 hauptsächlich von den Ransomware-Familien Locky, TeslaCrypt, Nemucod, CryptoWall, CTB-Locker und Petya betroffen.Seit Mai gibt es mit Cerber eine weitere in Deutschland häufig detektierte Ransomware-Familie.

Auch die Wirtschaft in Deutschland ist von Ransomware betroffen: Nach einer Umfrage des BSI waren ein Drittel der Unternehmen in den letzten sechs Monaten von Ransomware betroffen. Drei Viertel der Infektionen waren auf infizierte E-Mail-Anhänge zurückzuführen. Während 70 Prozent der betroffenen Unternehmen angaben, dass nur einzelne Arbeitsplatzrechner befallen waren, kam es in jedem fünften der betroffenen Unternehmen (22 Prozent) zu einem erheblichen Ausfall von Teilen der IT-Infrastruktur, 11 Prozent der Betroffenen erlitten einen Verlust wichtiger Daten.

Um eine Infektionen mit Ransomware zu verhindern oder einen eingetretenen Schaden zu minimieren, gibt es eine Vielzahl technischer sowie organisatorischer Maßnahmen in den Bereichen Prävention, Detektion und Reaktion, deren Umsetzung das BSI aufgrund der aktuellen Bedrohungslage empfiehlt. Dazu gehören vordringlich:

- Maßnahmen gegen die Angriffsvektoren Spam-E-Mails und Drive-by-Exploits, wie der Umgang mit Makros und Skripten in Office-Dokumenten oder Archiven oder das Patch-Management
- Ein unternehmensweites, regelmäßiges und funktionsfähiges Backup aller relevanten Daten
- Die Sensibilisierung der Mitarbeiter für die aktuellen Angriffsmethoden und Social Engineering
- Weitere Maßnahmen, um die Folgen einer Ransomware-Infektion abzumildern

Den aktuellen Kenntnisstand zum Thema Ransomware hat das BSI im vorliegenden Dossier zusammengestellt.

1 Ransomware

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes wieder freigeben. Der Name Ransomware ist ein Schachtelwort aus den englischen Begriffen ransom (deutsch: Lösegeld) und malware (deutsch: Schadprogramm). Grundsätzlich kann man Ransomware in zwei Kategorien einteilen:

- Ransomware, die den Zugang zu einem System sperrt oder unterbindet
- Ransomware, die Daten verschlüsselt.

Cyber-Angriffe durch Ransomware verletzen das Sicherheitsziel der Verfügbarkeit von Daten und Systemen. Gleichzeitig handelt es sich um eine Form digitaler Erpressung.

1.1 Historie

Ransomware ist kein neues Phänomen. Frühe Varianten und erste Konzepte für diesen Schadprogramm-Typ gab es bereits vor dem Jahr 2000 (https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf] [http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=502676). Erste einfache Varianten von Ransomware für Windows-Betriebssysteme wurden 2006 entdeckt. Diese verwendeten passwortgeschützte ZIP-Archive mit den Nutzerdaten des Opfers und verlangten ein Lösegeld für das Passwort des Archives[http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware21-ransomware21-ransomware21/).

Seit 2010 wird Ransomware verbreitet für Cyber-Angriffe eingesetzt. Die Ransomware-Familie Reveton wurde weltweit verwendet und hindert die Anwender durch eine Sperr-Nachricht auf dem Desktop an der Nutzung ihres Systems. Über eindringliche Warnungen und Aufforderungen wird behauptet, dass das System im Zuge polizeilicher oder sonstiger staatlicher Ermittlungen gesperrt sei und nur gegen Zahlung eines Bußgeldes oder Strafzahlung wieder freigegeben wird. Die Akteure nutzten für die Kampagnen unterschiedliche Namen und Logos polizeilicher oder sonstiger bekannter Organisationen. Je nach vermuteter Herkunft des Opfersystems wurden diese landesspezifisch angepasst. In Deutschland war dieser Typ wahlweise als BKA-, BSI- oder GVU-Trojaner bekannt.

Im September 2013 wurde mit CryptoLocker erstmalig eine Ransomware mit Verschlüsselungsfunktion breitflächig verwendet. Das Schadprogramm wählte Nutzerdateien bestimmten Typs aus und verschlüsselte diese mit symmetrischen und asymmetrischen Verfahren (AES256/RSA2048). Bereits damals wurden nicht nur Daten auf lokalen Festplatten verschlüsselt, sondern zusätzlich Daten von eingebundenen Netzwerklaufwerken erfasst.

1.2 Funktionsweise

Ransomware lässt sich grundsätzlich in zwei Kategorien einteilen:

- Ransomware, die den Zugang zu einem System sperrt oder unterbindet
- Ransomware, die Daten verschlüsselt.

1.2.1 Ransomware mit Sperrbildschirmen

Ransomware, die den Zugang zu einem System sperrt oder unterbindet, verankert sich im infizierten System, sodass die Ransomware nach jedem Systemstart geladen wird. Der Arbeitsplatz wird mit einem Bild oder einer Webseite überlagert, in der der Nutzer über die Sperrung des Systems informiert und zu einer Zahlung aufgefordert wird.

Als Ursache der Sperrung werden angebliche Verfahren wegen Verstößen gegen das Urheberrecht oder der Nutzung pornografischer Inhalte angegeben, deren Strafverfolgung gegen Zahlung einer angeblichen Strafe nicht weiterverfolgt und der Zugriff auf das infizierte System wieder ermöglicht wird.
Um der Forderung Nachdruck zu verleihen, werden Namen und Logos polizeilicher oder sonstiger Organisationen verwendet und mitunter auch pornografische Inhalte oder ein Bild einer angeschlossenen Webcam auf dem Sperrbildschirm angezeigt. Je nach Geolokation der IP-Adresse des Opfersystems werden die Sperrbildschirme landesspezifisch angepasst. In Deutschland war dieser Typ wahlweise als BKA-, BSI- oder GVU-Trojaner bekannt. Für die Lösegeldzahlung oder für die Zahlung der Sanktionsstrafe wird auf Guthabenkarten wie Paysafecard, Ukash oder auf auch kostenpflichtige SMS-Premiumdienste zurückgegriffen.

Technisch nutzen die Schadprogramme verschiedene Methoden, um sich im Autostart-Mechanismus des Betriebssystems zu verankern. Die einzig mögliche Interaktion mit dem System besteht darin, den Code einer Gutscheinkarte zur Zahlung einzugeben. Alle anderen Eingaben und Tastaturkombinationen werden abgefangen und ignoriert. Zusätzlich überprüft das Schadprogramm dauerhaft, ob weitere Prozesse gestartet werden, mit denen die Ransomware ggf. umgangen oder deaktiviert werden kann und beendet diese umgehend (Task-Manager, Registry-Editor, Eingabeaufforderung).

Da bei dieser Form von Ransomware nur die Ausführung des Systems beschränkt wird, kann das System mittels Virenschutzprogrammen oder Rettungssystemen, die mittels CD oder USB-Stick starten, wiederhergestellt werden, ohne dass es zu Datenverlusten für das Opfer kommt.

Eine ähnliche Funktionsweise hat die Ransomware Browlock. Hier wird nicht das Betriebssystem infiziert, sondern ausschließlich ein Sperrbildschirm im Vollbildmodus des Browsers angezeigt. Versuche des Nutzers das Fenster zu schließen und die Sperrseite zu umgehen, werden mittels JavaScript blockiert.

1.2.2 Ransomware mit Verschlüsselung

Ransomware, die Daten verschlüsselt, ist komplexer aufgebaut als Ransomware mit Sperrbildschirmen. Je nach Familie werden symmetrische und oder asymmetrische Verfahren zur Verschlüsselung der Daten genutzt oder kombiniert. Bei korrekter Implementierung der kryptografischen Primitiven ist die Wiederherstellung der verschlüsselten Daten nur mit dem passenden Schlüssel möglich. Im Gegensatz zu Ransomware mit Sperrbildschirm ist das Betriebssystem im Normalfall aber weiterhin nutzbar. Andere für diesen Typ Schadprogramm häufig verwendete Begriffe sind z.B. Krypto-Trojaner, Verschlüsselungs-Trojaner oder Cryptoware.

Die Verschlüsselung der Dateien erfolgt in der Regel mehrstufig:

1. Verschlüsselung der Dateien mit einem symmetrischen Verschlüsselungsverfahren, wie z.B. AES.
2. Verschlüsselung der symmetrischen Schlüssel mit einem asymmetrischen Verfahren, beispielsweise mittels RSA oder auf Elliptischen Kurven basierenden Verfahren (ECC).

Im nächsten Schritt sucht die Ransomware auf lokalen Laufwerken wie Festplatten und USB-Sticks sowie auf Netzlaufwerken nach Daten des Nutzers, wie z.B. Dokumenten und Tabellen, Fotos und Videos, sowie vielen weiteren Dateitypen, die für den Anwender einen hohen Wert haben. Viele Ransomware-Varianten enthalten dazu eine Liste von Datei-Typen, die verschlüsselt werden sollen.

.123 .3dm .3ds .3g2 .3gp .602 .7z .aes .arc .asc .asf .asm .asp .avi .bak .bat .bmp .brd .cgm .class .cmd .cpp .crt .cs .csr .csv .db .dbf .dch .dif .dip .djv .djvu .doc .docb .docm docx .dot .dotm .dotx .fla .flv .frm .gif .gpg .gz .hwp .ibd .jar .java .jpeg .jpg .js .key .lay .lay6 .ldf .m3u .m4u .max .mdb .mdf .mid .mkv .mml .mov .mp3 .mp4 .mpeg .mpg .ms11 .myd .myi .nef .odb .odg .odp .ods .odt .otg .otp .ots .ott .p12 .paq .pas .pdf .pem .php .pl .png .pot .potm .potx .ppam .pps .ppsm .ppsx .ppt .pptm .pptx .psd .qcow2 .rar .raw .rb .RTF .sch .sh .sldm .sldx .slk .sql .sqlite3 .Liedtitel .stc .std .sti .stw .svg .swf .sxc .sxd .sxi .sxm .sxw .tar .tar.bz2 .tbk .tgz .tif .tiff .txt .uop .uot .vb .vbs .vdi .vmdk .vmx .vob .wav .wb2 .wk1 .wks .wma .wmv .xlc .xlm .xls .xlsb .xlsm .xlsx .xlt .xltm .xltx .xlw .xml .zip

Liste von Dateitypen, die von der Ransomware Locky verschlüsselt werden (https://www.symantec.com/security_response/writeup.jsp?docid=2016-021706-1402-99&tabid=2)

Daneben gibt es ggf. eine weitere Liste von Dateien und Ordnern, die von einer Verschlüsselung ausgenommen werden, um auszuschließen, dass für den Betrieb des Systems notwendige Daten verschlüsselt werden.

Die unverschlüsselten Daten werden mit den verschlüsselten Kopien überschrieben oder nach der Verschlüsselung gelöscht. Im Anschluss wird der Nutzer über die Verschlüsselung seiner Daten informiert. Dazu werden Hinweistexte als Textdatei, Bilddatei oder in einem anderen Format auf dem System abgelegt oder als Hintergrund des Desktops angezeigt.

Ransomware-Familien die sich selbstständig und aktiv weiterverbreiten sind selten. Zwei Ausnahmen sind die Ransomware-Familien CryptoLocker und ZCryptor, die sich über externe Laufwerke wie z.B. USB-Medien weiterverbreiten.
In der Regel löscht sich das Schadprogramm selbstständig, nachdem die Verschlüsselung der Daten abgeschlossen ist.

1.2.3 Weitere Eigenschaften

Neben der zuvor beschriebenen grundsätzlichen Funktionsweise von Ransomware gibt es darüber hinaus weitere Funktionen oder spezifische Eigenschaften, die nur von einzelnen Ransomware-Familien genutzt werden. Der folgende Abschnitt zeigt einige dieser Funktionen.

Externe Medien und Netzlaufwerke

Viele Ransomware-Familien verschlüsseln neben lokalen Laufwerken auch angeschlossene externe Medien (z.B. USB-Sticks) sowie Netzlaufwerke. Gerade in Unternehmensnetzen mit weitreichenden Zugriffsmöglichkeiten können dadurch einzelne mit Ransomware infizierte Systeme unternehmensweite Datenverluste verursachen. Ransomware-Familien wie CryptoFortress, DMA-Locker sowie Locky verschlüsseln nicht nur Daten auf fest eingebunden Netzlaufwerken, sondern auf allen Netzlaufwerken, auf das das infizierte System Zugriff hat. Der Schaden durch eine Ransomware mit Verschlüsselung erstreckt sich damit auf alle Bereiche, die für das infizierte System zugreifbar sind. Gegebenenfalls können auch Daten auf eingebundenen Cloud-Speichern durch die Ransomware verschlüsselt werden.

Volumeschattenkopie und Systemwiederherstellung

Moderne Betriebssysteme enhalten Dienste, die im Hintergrund Versionsstände von Dateien oder der Systemkonfiguration festhalten. Im Fehlerfall helfen diese Dienste, frühere Versionen von Dateien oder eine lauffähige Systemkonfiguration wieder herzustellen. Für das Betriebssystem Microsoft Windows sind das beispielsweise:

- Volumeschattenkopie - Volume Shadow Copy Service (VSS) und die
- Systemwiederherstellung.

Bei einer Ransomware-Infektion sind diese Dienste jedoch keine Hilfe bei der Wiederherstellung der Daten: die Systemwiederherstellung beschränkt sich nur auf Dateien und Einstellungen, die für den Betrieb des Systems relevant sind, jedoch nicht auf die Nutzerdaten.

Alte und damit unverschlüsslte Versionsstände von Nutzerdateien, die durch die Volumeschattenkopie erstellt wurden, werden von vielen Ransomware-Familien (z.B. CryptoLocker, TeslaCrypt, Locky) gelöscht und stehen damit ebenfalls nicht mehr zur Verfügung.

Verschlüsselung auf Ebene des Dateisystems

Vereinzelte Ransomware-Familien agieren außerhalb des laufenden Betriebssystems und manipulieren dazu den Master Boot Record der Festplatte oder verschlüsseln Daten auf Partitionsebene. Beispiele:

- Ransomware-Typen wie Trojan-Ransom.Win32.Seftad.a oder TROJ_RANSOM.AQB tauschen den Master Boot Record (MBR) aus. Beim Booten des Systems wird ein Sperrbildschirm auf der Konsole angezeigt. Nach Zahlung des Lösegeldes wird der ursprüngliche MBR wiederhergestellt.
- Die Ransomware Petya schreibt sich in den MBR der Festplatte und startet das System neu. Anstatt des Bootloaders des Betriebssystems wird der Programmcode der Ransomware ausgeführt. Während dem Nutzer vermeintlich ein Programm zur Überprüfung der Festplatte angezeigt wird (CHKDSK), werden im Hintergrund die Daten der Master File Table (MFT) verschlüsselt. Nach Abschluss der Verschlüsselung wird dem Opfer ein Sperrbildschirm auf der Konsole angezeigt.

Lösegelderhöhung und Drohung mit Datenverlust

Um die Opfer von Ransomware unter Druck zu setzen und zu einer schnellen Zahlung eines Lösegeldes zu bewegen, werden unterschiedliche Methoden angewendet:

- Die Höhe der Lösegelder ist, in Relation zum Verlust der eigenen Daten, in den meisten Fällen als gering einzuschätzen.
- Stufenweise Erhöhung des Lösegeldes: Zahlt das Opfer nicht binnen eines vorgegebenen Zeitraums, so wird mit einer signifikanten Erhöhung der Lösegeldsumme gedroht (einmalige Erhöhung, z.B. Verdopplung oder stufenweise Steigerung der Lösegeldforderung nach Zeit).
- Dem Opfer wird ein Zeitraum vorgegeben, in dem das initial veranschlagte Lösegeld zu zahlen ist. Es wird damit gedroht, die Schlüssel nach Ablauf der Frist zu vernichten und die Wiederherstellung der Daten somit unmöglich zu machen.
- Es wird damit gedroht, pro Stunde Wartezeit eine feste Anzahl zufälliger Dateien zu löschen. Ein Neustart des Systems ist mit dem Verlust von 1000 Dateien verbunden.

1.2.4 Lösegeldzahlung

Ransomware ist für Cyber-Kriminelle ein seit Jahren etabliertes Geschäftsmodell. Aus der Sicht der Kriminellen haben Cyber-Angriffe mittels Ransomware den Vorteil, dass es zu einem direkten Geldtransfer zwischen Opfer und Täter über anonyme Zahlungsmittel wie Bitcoin oder Guthaben- und Bezahlkarten (Paysafecard, Ukash) kommt. In Einzelfällen wird eine Lösegeldzahlung auch über SMS-Premiumdienste oder Geschenkkarten-Codes (Apple iTunes, Amazon) verlangt. Im Vergleich zu Cyber-Angriffen über Banking-Trojaner sind weder Mittelsmänner für Überweisungen noch Waren-Agenten notwendig, um einen erfolgreichen Angriff zu Geld zu machen.

1.3 Plattformen

Der überwiegende Teil der bekannten Schadsoftware zielt auf das Betriebssystem Microsoft Windows. Ransomware ist dabei keine Ausnahme: Auch bei diesem Typ Schadprogramm greifen die meisten Familien und Varianten Nutzer dieses Betriebssystems an. Daneben gibt dennoch vereinzelte Ransomware-Familien, die auf das Desktop-Betriebssystem Apple MacOS X, Server-Systeme unter GNU/Linux als auch mobile Betriebssysteme wie Google Android abzielen. Erfolgreiche Angriffsmethoden der Windows-Plattform werden so auf andere Plattformen portiert. Die folgende Tabelle zeigt eine Auswahl:

Name	bekannt seit	Plattform	Ransomware -Typ	Merkmale
KeRanger	03/2016	MacOS X	Datei-Verschlüsselung	• servergenerierter öffentlicher RSA-Schlüssel je infiziertem System (RSA2048), individuelle symmetrische Verschlüsselung je Datei (AES256) • Verbreitung über einen manipulierten Installer des Bittorrent-Clients "Transmission". Der Nutzer muss diese betroffene Software installieren, um sich mit der Ransomware zu infizieren. • Installer-Datei war mit einem gültigen Entwickler-Zertifikat signiert, um Schutzmaßnahmen des Betriebssystems zu umgehen. • Lösegeld: 1 Bitcoin • Quellen: http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/ http://www.welivesecurity.com/2016/03/07/new-mac-ransomware-appears-keranger-spread-via-transmission-app/
FileCoder	06/2014	MacOS X	Datei-Verschlüsselung	• statische symmetrische Verschlüsselung (AES) • Entdeckung des Samples auf VirusTotal. • unfertige Version des Schadprogramms ohne Verschlüsselung von Nutzerdaten • Lösegeld: 20 - 30 € via Paypal/Western Union/Kreditkarte • Quellen: https://securelist.com/blog/research/66760/unfinished-ransomware-for-macos-x/

Name	bekannt seit	Plattform	Ransomware -Typ	Merkmale
Linux.Encoder	11/2015	GNU/Linux	Datei-Verschlüsselung	• Infektionen mit der Ransomware stehen in Zusammenhang mit System, die über Schwachstellen im Shopsystem Magento infiziert wurden. • Version 1-3 der Ransomware hatte eine Schwäche in der Implementierung der symmetrischen Verschlüsselung, wodurch es möglich war, verschlüsselte Daten wiederherzustellen. • Laut Bitdefender hat Linux.Encoder starke Ähnlichkeiten zu KeRanger. • Quellen: https://labs.bitdefender.com/2016/03/keranger-is-actually-a-rewrite-of-linux-encoder/ https://labs.bitdefender.com/2015/11/linux-ransomware-debut-fails-on-predictable-encryption-key/
CTB-Locker (Webserver)	02/2016	GNU/Linux	Datei-Verschlüsselung	• Verschlüsselung mit AES256 • Lösegeld: Anfangs 0,4 Bitcoin, mit der Zeit mehr • Nach Infektion wird die Startseite des Webservers (index.html) oder ähnlich gegen eine index.php Datei ausgetauscht, die die Daten verschlüsselt und die Erpresser-Nachricht beim Aufruf der Seite anzeigt. • Das Opfer kann zwei zufällig ausgewählte Dateien kostenlos entschlüsseln. Diese sind jedoch mit einem anderen Schlüssel verschlüsselt als die anderen Daten • Quellen http://www.heise.de/security/meldung/Admins-aufgepasst-Krypto-Trojaner-befaellt-hunderte-Webserver-3116470.html http://www.bleepingcomputer.com/news/security/ctb-locker-for-websites-reinventing-an-old-ransomware/

Android Defender /FakeAV.B.	Mitte 2013	Android	Sperr-Bildschirm	• Das Schadprogramm tarnt sich als Sicherheits-App und hat ein zweistufiges Vorgehen:
				  • Phase 1: Anzeigen von vorgetäuschten Schadprogramm-Infektionen (Pop-Up), die gegen Zahlung bereinigt werden sollen.
				  • Phase 2: 6h nach Infektion folgt die Anzeige eines dauerhaften Sperrbildschirms mit pornografischen Inhalt, der gegen Zahlung bereinigt werden soll.
				• Lösegeld 100 US$ per Kreditkarte
				• Quellen: http://www.welivesecurity.com/2016/02/18/the-rise-of-android-ransomware/

Name	bekannt seit	Plattform	Ransomware -Typ	Merkmale
Koler	Mai 2014	Andorid	Sperr-Bildschirm	• Das Schadprogramm wird dem Nutzer als benötige Software zum Abspielen von Videos auf einer Webseite angeboten. Die Installation erfolgt nach Bestätigung durch den Nutzer. • Der Homescreen des Gerätes wird mit einem Sperrbildschirm überlagert und dem Nutzer eine Straftat unterstellt. Nach Zahlung einer Strafe soll die Nutzung des Gerätes wieder möglich sein. Anhand der Geolokation der IP-Adresse des Geräts wählt das Schadprogramm einen zu den Strafverfolgungsbehörden des Landes gehörenden Sperrbildschirm. • Lösegeld: 300 € • Quellen: https://labs.bitdefender.com/2014/05/reveton-icepol-ransomware-moves-to-android/
Simplocker	Juni 2014	Andorid	Datei-Verschlüsselung	• Erste Ransomware für Android mit Datei-Verschlüsselung • Verschlüsselung mit einem im Programmcode hinterlegten statischen AES-Schlüssel. Zur Wiederherstellung von Daten stehen kostenfreie Tools zur Verfügung. • Erste Version des Schadprogramms mit osteuropäischen Sprachen, später eine Variante auf Englisch. • Lösegeld: 16 € • Quellen: http://www.welivesecurity.com/2014/06/04/simplocker/

Tabelle 1: Beispiele für Ransomware-Familien für die Plattformen Apple MacOS, GNU/Linux und Google Android

1.4 Verschlüsselung

Ransomware mit Verschlüsselung setzt heute auf kryptografisch starke Algorithmen. Bei der korrekten Verwendung und Implementierung dieser Algorithmen ist eine Entschlüsselung der Daten ohne den passenden Schlüssel unmöglich.
Heute werden vorwiegend Kombinationen aus symmetrischen Verfahren (zur Datenverschlüsselung) und asymmetrischen Verfahren (zum Schlüsselaustausch) eingesetzt.

Nach der initialen Infektion wird entweder ein asymmetrisches Schlüsselpaar generiert, die benötigten Schlüssel durch einen Steuerungsserver bereitgestellt oder die öffentlichen Schlüssel sind bereits Bestandteil des Schadprogramms. Häufig sind die Schlüssel dem betroffenen System zugeordnet. Der private Schlüssel wird auf dem Steuerungsserver des Angreifers hinterlegt und ermöglicht eine Entschlüsselung der Daten nach Zahlung des Lösegelds.

Je nach Art des Schlüsselaustausches ist eine Verbindung zum Steuerungs-Server zum Zeitpunkt der Infektion Voraussetzung für die Verschlüsselung der Daten. Ransomware-Familien die einen öffentlichen Schlüssel im Schadprogramm beinhalten sind nicht auf eine Internetverbindung und einen Schlüsselaustausch mit einem Steuerungs-Server angewiesen.

Folgende kryptografische Verfahren wurden oder werden für Ransomware verwendet:

- RSA (1024 - 4096 Bit Schlüssellänge)
- ECDH (u.a.192 Bit Schlüssellänge)
- AES (128 - 256 Bit Schlüssellänge)
- RC4
- Salsa20

Für manche Ransomware-Familien steht mittlerweile ein öffentliches Tool zum Entschlüsseln der Daten zur Verfügung. Nach Kenntnis des BSI gibt es aktuelle Entschlüsselungs-Tools für die folgenden Ransomware-Familien:

Ransomware-Familie	Datum	Link
Harasom	18.08.2013	https://decrypter.emsisoft.com/harasom
CryptoDefense	02.04.2014	https://decrypter.emsisoft.com/cryptodefense
TorLocker / Scraper	08.04.2015	https://securelist.com/blog/research/69481/a-flawed-ransomware-encryptor/
PCLock	29.04.2015	https://decrypter.emsisoft.com/pclock
TeslaCrypt 1.0 / AlphaCrypt	13.05.2015	http://www.bleepingcomputer.com/virus-removal/teslacrypt-alphacrypt-ransomware-information#decrypt
CoinVault / Bitcryptor	28.10.2015	https://noransom.kaspersky.com/
Linux Encoder	10.11.2015	https://labs.bitdefender.com/2015/11/linux-ransomware-debut-fails-on-predictable-encryption-key/
CryptInfinite	22.11.2015	https://decrypter.emsisoft.com/cryptinfinite
Rakhni	11.12.2015	http://support.kaspersky.com/de/viruses/disinfection/10556
Radamant	02.01.2016	https://decrypter.emsisoft.com/radamant
TeslaCrypt 2.0	20.01.2016	https://up2sha.re/GGTSPU-fw1.bsi.bund.de-32760-6546225-xMh9MxnlcLkeofgD-DAT/file?l=C5ag0MrQNqAb.pdf
KeyBTC	24.01.2016	https://decrypter.emsisoft.com/keybtc
LeChiffre	25.01.2016	https://decrypter.emsisoft.com/lechiffre
Gomasom	25.01.2016	https://decrypter.emsisoft.com/gomasom
CrypBoss	30.01.2016	https://decrypter.emsisoft.com/crypboss
DMALocker	06.02.2016	https://decrypter.emsisoft.com/dmalocker
HydraCrypt	12.02.2016	https://decrypter.emsisoft.com/hydracrypt
DMALocker2	18.02.2016	https://decrypter.emsisoft.com/dmalocker2
Nemucod	22.03.2016	https://decrypter.emsisoft.com/nemucod
Petya	09.04.2016	https://github.com/leo-stone/hack-petya/blob/master/README.md
Jigsaw/CryptoHitman	11.04.2016 11.05.2016	http://www.bleepingcomputer.com/news/security/jigsaw-ransomware-decrypted-will-delete-your-files-until-you-pay-the-ransom/ http://www.bleepingcomputer.com/news/security/jigsaw-ransomware-becomes-cryptohitman-with-porno-extension/
AutoLocky (nicht die in DE verbreitete Familie Locky)	16.04.2016	https://decrypter.emsisoft.com/autolocky

Ransomware-Familie	Datum	Link
CryptXXX	26.04.2016	https://blog.kaspersky.com/cryptxxx-ransomware/11939/
Alpha	30.04.2016	http://www.bleepingcomputer.com/news/security/decrypted-alpha-ransomware-accepts-itunes-gift-cards-as-payment/
TeslaCrypt 3 - 4	18.05.2016	http://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/ http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/

Tabelle 2: Liste bekannter Entschlüsselungs-Tools für Ransomware

Trotz der Vielzahl der Entschlüsselungstools kann nicht davon ausgegangen werden, dass für jede Familie oder neue Variante kurzfristig ein Tool zur Entschlüsselung der Daten veröffentlicht wird. Gerade für die in Deutschland in den letzten Monaten großflächig aktive Ransomware-Variante Locky ist dem BSI aktuell kein Tool zur Entschlüsselung der Daten bekannt.

2 Bedrohungslage

Ransomware ist kein neues Phänomen. Spätestens mit dem Auftreten von Ransomware mit Sperrbildschirmen im Jahr 2011 handelt es sich um eine weitverbreitete Form von Schadprogramm sowie um ein etabliertes Geschäftsmodell im Bereich der Cyber-Kriminalität. Durch die Weiterentwicklung von Ransomware mit Sperrbildschirm zu Ransomware mit Verschlüsselungsfunktion sind die Auswirkungen auf die Betroffenen heute jedoch drastischer.

Ein von Sicherheitsforschern bereitgestelltes Tool zur Identifikation von Ransomware-Familien enthielt Ende Mai 2016 mehr als 100 unterschiedliche Familien von Ransomware mit Verschlüsselungsfunktion (https://id-ransomware.malwarehunterteam.com/).

Nach Auswertung der dem BSI vorliegenden Daten war Deutschland im ersten Quartal 2016 hauptsächlich von den Ransomware-Familien

- Locky
- TeslaCrypt
- Nemucod
- CryptoWall
- CTB-Locker
- Petya

betroffen. Seit Mai gibt es mit Cerber eine weitere in Deutschland häufig detektierte Ransomware-Familie.

Die Daten zeigen auch, dass es sich heute überwiegend um Angriffe von Ransomware mit Verschlüsselungsfunktion handelt. Die einfachen Varianten von Ransomware mit Sperrbildschirm haben heute im Bereich der Desktop-Betriebssysteme keine Relevanz mehr.

Beim überwiegenden Teil der Angriffe handelt es sich um ungezielte Massenangriffe. Dennoch gibt es daneben auch einzelne Ransomware-Familien sowie Berichte über Vorfälle, die auf ein gezieltes bzw. manuelles Vorgehen bei der Infektion mit Ransomware schließen lassen.

Dem BSI vorliegende Detektionszahlen von Virenschutz-Produkten in Deutschland zeigen, dass sich die Bedrohungslage durch Ransomware in Deutschland seit Herbst 2015 verschärft hat (Abbildung 1). Eine Auswertung der Detektionsdaten von Virenschutzprogrammen für Deutschland zeigt, dass die Detektionen für den Angriffsvektor E-Mail (Spam-E-Mails mit Anhängen, die mit Ransomware in Verbindung stehen) in Deutschland zwischen Januar und Mai 2016 um Faktor 70 angestiegen sind. Dagegen sind seit Februar die AV-Detektionen für aktive Ransomware und entdeckte Infektionen auf Client-Systemen nahezu konstant geblieben.

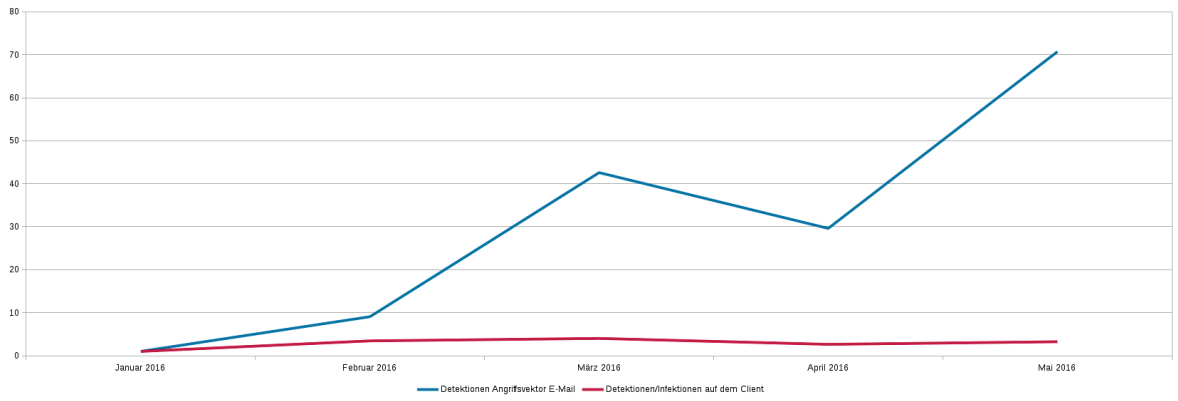

Abbildung 1: Anstieg der Ransomware-Detektionen von Virenschutzprogrammen in Deutschland seit Januar 2016

2.1 Angriffsvektoren

Die häufigsten Angriffsvektoren, über die Client-Systeme mit Ransomware infiziert werden, sind Anhänge von Spam-E-Mails sowie Drive-By-Angriffe mittels Exploit Kits. Server-Systeme werden durch das Ausnutzen von Software-Schwachstellen mit Ransomware infiziert. Die unterschiedlichen Angriffsvektoren von Ransomware werden im folgenden Abschnitt vorgestellt.

2.1.1 Angriffsvektor Spam

Massenhaft versendete Spam-E-Mails gehören zu den am häufigsten zu beobachtenden Angriffsvektoren von Ransomware. Die Spam-E-Mails enthalten beispielsweise angebliche Rechnungen, Bestellbestätigungen, Paketlieferungen, eingescannte Dokumente, Bewerbungsschreiben, Fax-Nachrichten oder angebliche Fotos. Dabei werden Absender-Namen von bekannten oder unbekannten Unternehmen sowie von Privatpersonen verwendet. Eine abschließende Auflistung ist nicht möglich, da täglich neue Angriffswellen mit neuen Varianten von Anschreiben verwendet werden.

Über dieses Social Engineering sollen die Empfänger der Nachrichten dazu verleitet werden, den Anhang der E-Mails zu öffnen. Die Typen der als Anhang versendeten Dateien ändern sich stetig. Beobachtet werden:

- Office-Dokumente oder Vorlagen (.doc/.xls .docx/.xlsx .docm .dot) mit Makros
- Archiv-Dateien mit oder ohne Passwort-Schutz (.zip .rar)
- Script-Dateien wie JavaScript, VisualBasicScript oder PowerShell-Scripte (.js .vbs .ps1 .wsf)
- Programmdateien (.exe), die z.B. mit einem PDF-Icon als Dokument getarnt sind
- Script-Dateien mit mehreren Dateiendungen, wie script.pdf.js. Ist die Anzeige der Dateiendung deaktiviert (Standardeinstellung bei Microsoft Windows), wird suggeriert, dass es sich um ein Dokument und kein Script handelt.
- Kombinationen der oben genannten, z.B. Script- oder Programmdateien in einem Archiv, oder Word-Makros die ein PowerShell-Script ausführen

Der Anhang enthält in den meisten Fällen nicht das Schadprogramm selbst, sondern agiert als sogenannter Downloader oder Dropper. Erst nach dem Öffnen oder Ausführen des Droppers wird das eigentliche Schadprogramm nachgeladen und ausgeführt.
Im Fall von JavaScript oder VisualBasicScript erfolgt die Ausführung über Funktionen der Script-Sprache in der Laufzeitumgebung (Windows Script Host). Bei Office-Dokumenten wird ein eingebetteter und ggf. stark verschleierter Makro-Code verwendet, um das Schadprogramm herunterzuladen und auszuführen. In den

Dokumenten können zusätzliche Hinweise enthalten sein, die den Nutzer auffordern, etwaige Warnmeldungen oder Abfragen vor Ausführung eines Makros zu bestätigen, da dies zur korrekten Anzeige des Dokuments notwendig sei.
In der Vergangenheit wurden auch Kampagnen beobachtet, in denen die Schadsoftware direkt verteilt wurde, z. B. als Programmdatei (.exe) in einem Archiv oder eingebettet in einem Office-Dokument.

Durch das Zwischenschalten eines Droppers vor dem Herunterladen des tatsächlichen Schadprogramms bleiben das dahinterliegende Verteilungsnetz als auch die Angreifer flexibel: So kann immer die aktuellste Version eines Schadprogramms ausgeliefert oder das Schadprogramm dynamisch ausgetauscht werden, z.B. bei einer - aus Sicht der Angreifer - zu guten Erkennung durch Virenschutzprogramme.

Darüber hinaus kann der Programm-Code der Dropper beliebig geändert werden, z.B durch das Anhängen von Zufallswerten in einem Archiv oder der Umbenennung von Variablen in einem Script, ohne dessen Funktion zu beeinträchtigen. Eine Erkennung des Schadprogramms durch Hashwert-basierte Komponenten von Virenschutzprogrammen wird so verhindert.

Ausgangspunkt der Spam-Wellen sind z.B. Botnetze, wie das für die Verteilung von Banking-Trojanern bekannte Spamnetzwerk DRIDEX, das seit Monaten die größte Quelle von Spam-Nachrichten mit Schadsoftware im Anhang ist. Bereits im Dezember 2015 beobachtete das BSI große Spam-Wellen mit Anhängen, die bei Ausführung eine Infektion mit Ransomware, vorwiegend TeslaCrypt, zur Folge hatten. Ab Mitte Februar 2016 wurde DRIDEX für die Verteilung von Droppern verwendet, die die Ransomware Locky nachgeladen haben.

Abbildung 2 zeigt den qualitativen Verlauf der Detektionen von Virenschutzprogrammen (Client- und Server-Systeme) für Office-Dokumente mit eingebetteten Makros im 1. Quartal 2016 in Deutschland, die entweder mit dem DRIDEX-Botnetz oder Infektionen mit der Ransomware Locky in Zusammenhang stehen[1]. Neben den ausgeprägten Wellen zum Monatswechsel Januar/Februar sowie Mitte Februar 2016 wird deutlich, dass Nutzer in Deutschland über das gesamte Quartal hinweg von Angriffen durch DRIDEX betroffen waren, und nicht erst seit Beginn des großflächigen Auftretens der Ransomware Locky Mitte Februar.

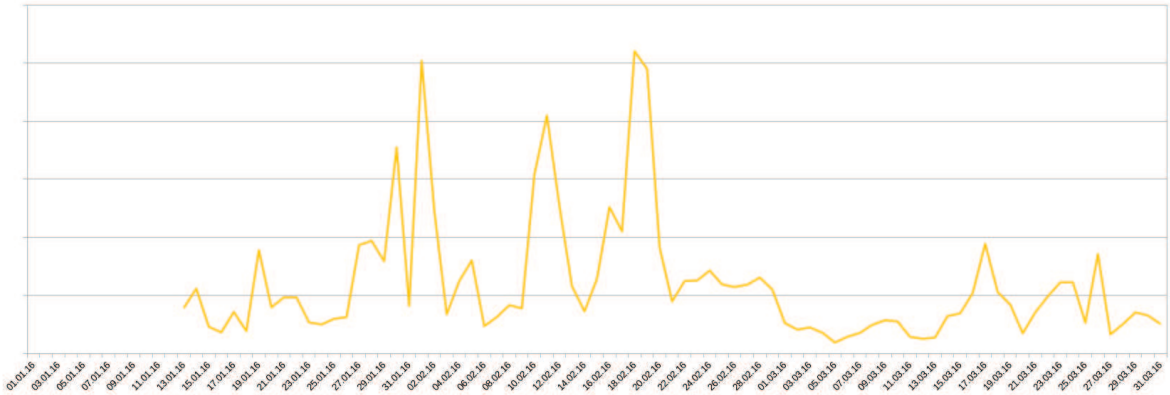

Abbildung 2: AV-Detektionen für Office-Dokumente mit eingebetteten Makros in Q1/2016 in Deutschland, die mit dem DRIDEX-Botnetz oder der Ransomware Locky zusammenhängen

Abbildung 3 zeigt den Verlauf der von Januar - Mai 2016 vom BSI analysierten Schadprogramm-Samples aus Spam-Mails (einzigartige Samples) nach Ransomware-Familien. Über den gesamten Zeitraum fielen 57 Prozent der ausgewerteten Samples auf die Ransomware Locky, 26 Prozent auf TeslaCrypt, 10 Prozent auf die Ransomware Nemucod und 6 Prozent auf Cerber. Im Monat Mai gab es mehrere Spam-Wellen, deren Anhänge zu Infektionen mit Locky sowie Cerber führten. Im Gegensatz zu den Vormonaten wurde TeslaCrypt im Mai nicht mehr per Spam-E-Mail verteilt. Diese Beobachtung passt zur Veröffentlichung eines Masterschlüssels zur Entschlüsselung aller TeslaCrypt-Varianten Mitte Mai 2016.

1 Für den Zeitraum 01.01. - 12.01.16 stehen keine Daten zur Verfügung.

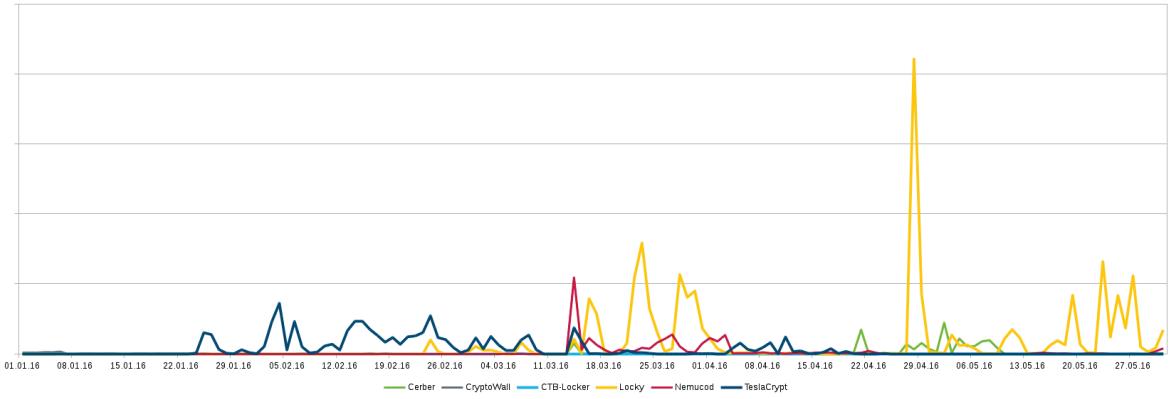

Abbildung 3: Verlauf der in Q1/2016 vom BSI analysierten Samples aus Spam-E-Mails nach Ransomware-Familien

Der schnelle Wechsel auf neue Ransomware-Familien konnte im Februar anhand der Weiterentwicklung von TeslaCrypt beobachtet werden: Wie Abbildung 4 zeigt, wurde bis zum 12./13. Februar ausschließlich TelsaCrypt in der Version 3.0 verteilt. Nach diesem Datum wurde bei der Auswertung der Anhänge von Spam-Mails nur noch TeslaCrypt in Version 4.0 detektiert.

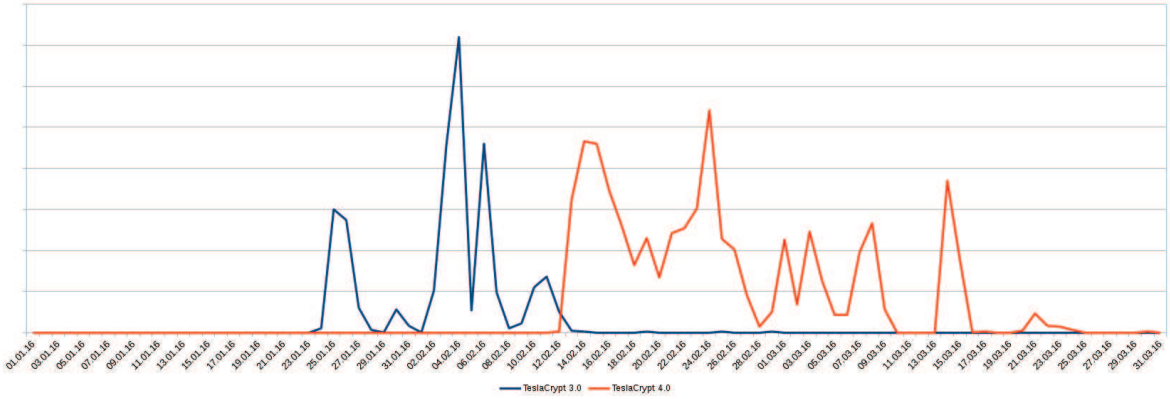

Abbildung 4: Verlauf der in Q1/2016 vom BSI analysierten Samples aus Spam-E-Mails für die Ransomware-Familien TeslaCrypt 3.0 und 4.0.

2.2 Angriffsvektor Drive-by-Angriffe mittels Exploit Kits

Exploit-Kits sind Angriffswerkzeuge, die mithilfe verschiedener Drive-by-Exploits versuchen, eine Schwachstelle auf einem Client-System zu finden und zur Installation von Schadprogrammen auszunutzen. Dazu werden kontinuierlich Exploits für neue Software-Schwachstellen in weit verbreiteten Programmen in Exploit-Kits integriert.

Nach Umleitung auf ein Exploit-Kit (mittels iframe oder schädlichem Werbebanner) werden im Hintergrund ohne Kenntnis oder Mitwirken des Nutzers vorhandene Schwachstellen im Webbrowser, in Browser-Plug-ins oder im Betriebssystem ausgenutzt, um Schadprogramme auf dem System zu installieren. Exploit-Kits gehören seit mehreren Jahren zu den Infektionsvektoren für Ransomware.

In Deutschland geht von den Exploit-Kits

- Angler
- Nuclear
- Magnitude
- Rig
- Neutrino

die meiste Aktivität aus. Alle genannten Exploit-Kits wurden in der Vergangenheit auch zur Installation von Ransomware verwendet.

Eine Auswahl aktueller Fälle, in denen Exploit-Kits zur Verbreitung von Ransomware verwendet wurden, ist hier dokumentiert:

Exploit-Kit	Ransomware-Familie	Quelle
Nuclear	Locky, TelsaCrypt	http://blog.checkpoint.com/2016/04/20/inside-nuclears-core-analyzing-the-nuclear-exploit-kit-infrastructure/
Magnitude	Cerber	https://blog.malwarebytes.org/cybercrime/2016/04/magnitude-ek-malvertising-campaign-adds-fingerprinting-gate/
Angler	CryptXXX	https://www.proofpoint.com/us/threat-insight/post/cryptxxx-new-ransomware-actors-behind-reveton-dropping-angler

Tabelle 3: Beispiele für Ransomware-Infektionen über Exploit-Kits

Ende April 2016 wurde bekannt, dass erstmals mobile Endgeräte mit Betriebssystem Google Android durch einen Exploit-Kit-Angriff beim Besuch einer Webseite mit Ransomware mit Sperrbildschirm infiziert wurden (https://www.bluecoat.com/security-blog/2016-04-25/android-exploit-delivers-dogspectus-ransomware). Bisherige Schadsoftware-Infektionen von Android-Systemen waren auf gefälschte Apps in App-Stores oder die manuelle Installation des Schadprogramms durch den Nutzer zurückzuführen.

2.3 Angriffsvektor Schwachstellen in Server-Software

Serversysteme unter Linux sind heute ebenfalls Ziel von Ransomware-Angriffen. Als Angriffsvektor dienen hier Schwachstellen in der auf dem Server eingesetzten Software. Für Infektionen mit der Ransomware-Familie Linux.Encoder wurden Schwachstellen im Shopsystem Magento ausgenutzt (https://labs.bitdefender.com/2015/11/linux-ransomware-debut-fails-on-predictable-encryption-key/). Für die Webserver-Ransomware CTB-Locker wird vermutet, dass dessen Infektionen auf Schwachstellen der Server-Software (https://securelist.com/blog/research/73989/ctb-locker-is-back-the-web-server-edition/) oder des Content Management Systems WordPress zurückzuführen sind (http://www.bleepingcomputer.com/news/security/ctb-locker-for-websites-reinventing-an-old-ransomware/).

2.4 Nachladen von Ransomware bei bestehenden Schadsoftware-Infektionen

Ist ein System mit Schadsoftware wie einem Bot oder einem Trojanischen Pferd infiziert, steht das System vollständig unter der Kontrolle des Angreifers. Bleibt die Infektion unentdeckt, kann das System beispielsweise zum Versand von Spam-Nachrichten, für DDoS-Angriffe oder zur Manipulation von

Online-Banking missbraucht werden. Weiterhin ist es möglich, über die bestehende Infektion weitere beliebige Schadprogramme nachzuladen. So kanndas System auch mit einer Ransomware infiziert werden . Ein Angreifer kann die bestehende Schadsoftware-Infektion dadurch auf neue Art monetarisieren.

Im April 2016 wurde mit dem Exploit-Kit Angler das Schadprogramm Bedep verteilt, was zum Click-Betrug verwendet wird. Nachdem das initiale Schadprogramm überprüft hat, dass es sich bei dem infizierten System nicht um eine virtuelle Maschine handelt, wurde zusätzlich die Ransomware CryptXXX nachgeladen (http://researchcenter.paloaltonetworks.com/2016/04/afraidgate-major-exploit-kit-campaign-swaps-locky-ransomware-for-cryptxxx/).

2.5 Angriffsvektoren manuelle bzw. gezielte Cyber-Angriffe mit Ransomware

Der überwiegende Anteil der Ransomware-Infektionen ist auf ungezielte Cyber-Angriffe zurückzuführen. Dennoch gibt es vereinzelte Berichte, in denen Organisationen gezielt oder zumindest durch einen manuellen Angriff Opfer von Ransomware und Erpressung wurden.

- Laut einem Medienbericht wurden Ende 2012 von einem Unternehmen der Gesundheitsbranche in Australien 4000 AU$ erpresst, nachdem die Täter in Systeme eindrangen und Patientendaten verschlüsselten (http://www.abc.net.au/news/2012-12-10/hackers-target-gold-coast-medical-centre/4418676).
- Bei Vorfällen mit der Ransomware GPCode wurde in einigen Fällen festgestellt, dass die Infektionen auf ungeschützte Fernwartungszugänge zurückzuführen war. Durch einen Brute-Force-Angriff auf das Passwort erlangten die Täter initialen Zugriff. Nach dem erfolgreichen Login wurden verschiedene Systeme mit der Ransomware infiziert.Zur Vorbereitung solcher Angriffe wird das Internet aktiv nach ungeschützten Fernwartungszugängen, wie beispielsweise Microsoft Remote-Desktop, durchsucht (Portscan).

  Neben den dem BSI bekannten Vorfällen gibt es auch öffentliche Berichte über weitere Angriffe, bei denen Unternehmen nach Brute-Force-Angriffen über RDP mit Ransomware infiziert und erpresst wurden (https://blog.fox-it.com/2016/05/02/ransomware-deployments-after-brute-force-rdp-attack/).
- Mehrere Sicherheitsdienstleister berichteten im März 2016 über Angriffskampagnen der Ransomware SamSam/Samas. Bei diesen Angriffen gelang der initiale Zugriff auf das interne Unternehmensnetzwerk über Software-Schwachstellen in JBoss-Anwendungs-Servern. In der Folge weiteten sie den Zugriff auf Systeme mit Microsoft Windows aus. Neben dem Verschlüsseln der Nutzerdaten und dem Löschen ggf. vorhandener Schattenkopien wurden Prozesse von Backup-Software beendet und Backup-Dateien gelöscht.

2.6 Betroffenheit der deutschen Wirtschaft durch Ransomware

Das BSI hat im April 2016 im Rahmen der Allianz für Cyber-Sicherheit eine Umfrage zur Betroffenheit der deutschen Wirtschaft durch Ransomware durchgeführt und fast 600 Rückmeldungen ausgewertet. Demnach war ein Drittel (32 Prozent) der antwortenden Unternehmen aller Größenordnungen in den letzten sechs Monaten von Ransomware betroffen. Die Mehrheit der an der Befragung beteiligten Unternehmen (60 Prozent) schätzt die Bedrohungslage für die eigene Institution als verschärft ein.

Drei Viertel (75 Prozent) der Infektionen waren auf infizierte E-Mail-Anhänge zurückzuführen. 17 Prozent gaben an, dass die Ransomware-Infektion auf einen Drive-by-Angriff zurückzuführen war. Die Zahlen bestätigen die bisherige Einschätzung des BSI zu den Angriffsvektoren von Ransomware. Die sich aus der Befragung ergebende Verteilung der Ransomware-Familien deckt sich auch mit den im BSI vorliegenden Daten weiterer Quellen: Die Unternehmen in Deutschland nannten am häufigsten Infektionen mit den

Ransomware-Familien Locky (37 Prozent), TeslaCrypt (29 Prozent), CryptoWall (10 Prozent) und CTB-Locker (9 Prozent). 11 Prozent gaben an, von sonstiger Ransomware betroffen gewesen zu sein.

Fast alle Unternehmen (86 Prozent) haben zusätzliche Maßnahmen getroffen, um sich besser vor Ransomware zu schützen. Dazu zählen die verstärkte Sensibilisierung der Mitarbeiter (76 Prozent) sowie technische Maßnahmen in Bereichen wie der Filterung an Netzübergängen, der Abwehr von Spam-Mails und der Verbesserung der Virenerkennung. 38 Prozent der Befragten planen überdies zusätzliche Maßnahmen im Bereich Datensicherung und Backups.

Zu einem vergleichbaren Ergebnis kommt eine Abfrage des BSI im KRITIS-Sektor Gesundheit, für die knapp 90 Rückmeldungen vorliegen:

Hier gaben 41 Prozent der Befragten an, dass es zu einer Infektion mit Ransomware in Folge eines Angriffs per E-Mail gekommen ist. Bei 39 Prozent der Befragten wurden Angriffsversuche durch ein Virenschutzprogramm abgefangen. Im Hinblick auf Schäden konnten in 95 Prozent der Fälle Daten binnen Stunden wiederhergestellt werden. Bei 3 Prozent der Befragten kam es zu einem Datenverlust, da die Wiederherstellung betroffener Daten nicht möglich war. Für 9 Prozent hatte die Ransomware-Infektion einen Ausfall bzw. eine Beeinträchtigung des Geschäftsbetriebs oder der Dienstleistung zur Folge.

Vor dem Hintergrund dieser Abfrage und dem bestehenden Informationsaustausch sieht das BSI keine erhöhte Bedrohung durch Ransomware für Unternehmen im Sektor Gesundheit.

In Ergänzung zu den zwei Umfragen hat das BSI durch Meldungen betroffener Unternehmen Kenntnis über weitere Ransomware-Infektionen in den Bereichen Gesundheit, Versicherung, Verkehr sowie Wasserver- und entsorgung in Deutschland.

2.7 Schäden

Anders als Infektionen mit Banking-Trojanern oder Bots führen Infektionen mit Ransomware zu direkten, unmittelbar erkennbaren Schäden und zu konkreten Konsequenzen bei den Opfern. Da infolge der Infektion Systeme und Daten nicht mehr zur Verfügung stehen, entsteht bei den Betroffenen, egal ob Privatpersonen oder Unternehmen und Behörden, ein hoher Leidensdruck.

2.7.1 Schäden für Privatpersonen

Da die Digitalisierung alle Lebensbereiche umfasst, sind heute auch auf privaten Systemen eine Vielzahl von Daten gespeichert, die nach einer Infektion mit Ransomware nicht mehr zur Verfügung stehen. Die Verschlüsselung von Adressbüchern, E-Mails, Schriftverkehr aller Art, digitalen Erinnerungsstücken wie Fotos und Videos, Musiksammlungen, Steuerdaten oder beruflichen Dokumenten wie Arbeitszeugnissen stellt auch für Privatpersonen einen großen praktischen wie emotionalen Verlust dar.

Im Vergleich zum Verlust solcher ideellen Werte können die Kosten für das Lösegeld bei manchen Betroffenen als gering angesehen werden, was die Bereitschaft zur Zahlung eines Lösegelds erhöht und den Erfolg des Geschäftsmodells Ransomware sicherstellt. Folglich sind auch im privaten Bereich präventive Maßnahmen wie ein regelmäßiges und zuverlässiges Backup zwangsläufig erforderlich, auch vor dem Hintergrund, dass ein Datenverlust nicht nur durch eine Ransomware-Infektion, sondern auch in Folge eines Defekts, Fehlbedienung oder Diebstahls eintreten kann.

2.7.2 Schäden für Organisationen

Schäden für eine Organisation durch Cyber-Sicherheitsvorfälle lassen sich grundsätzlich in

- Eigenschäden,
- Reputationsschäden,
- und Fremdschäden

unterteilen. Je nach Auffassung werden auch Kosten von allgemeinen Präventionsmaßnahmen oder Folgekosten nach einen Angriff, z. B. die Verbesserung der Organisations- oder IT-Struktur, dazu gezählt.

Zu den Eigenschäden gehören Kosten durch Betriebsbeeinträchtigungen bzw. -unterbrechungen der gesamten Organisation, wenn z. B. eine Produktion oder Dienstleistung in Folge eines Cyber-Angriffs nicht aufrechterhalten werden kann. Weiterhin können Kosten der Bereiche Krisenreaktion und -beratung durch Mitarbeiter oder externe Experten auftreten. Forensik und Wiederherstellung verursachen weitere Kosten. Aufgrund gesetzlicher Vorgaben sind des Weiteren Kosten für die Benachrichtigung von Betroffenen oder Aufsichtsbehörden sowie Bußgelder möglich.

Reputationsschäden ergeben sich für eine Organisation, wenn in Folge eines Angriffs das Ansehen der Organisation sinkt oder Kunden abwandern und so wirtschaftliche Nachteile entstehen (z. B. fallende Aktienkurse). Um die Reputation wieder aufzubauen, muss unter Umständen neu in Werbung, Kundenbindung und Imagebildung investiert werden.

Fremdschäden treten auf, wenn gesetzliche, vertragliche oder anderweitige Verpflichtungen gegenüber Dritten aufgrund eines Vorfalls nicht oder nicht vollständig erfüllt werden können (Verletzung der Vertraulichkeit, Nichteinhaltung vereinbarter Materialabnahmen oder Liefertermine sowie Produktmängel). Insbesondere bei Kritischen Infrastrukturen können die Fremdschäden potenziell sehr hoch sein.

Die Kostenschätzung von Cyber-Sicherheitsvorfällen ist von den individuellen Rahmenbedingungen einer Organisation und deren Gefährdungen abhängig. Ein erfolgreicher Angriff mit Ransomware kann Schäden in allen der drei genannten Kategorien zur Folge haben. Eine belastbare Aussage zu den konkreten direkten und indirekten Kosten, die durch eine Ransomware-Infektion entstehen, lässt sich aus den dem BSI vorliegenden Informationen nicht ableiten.

Das konkrete Schadensausmaß ist erheblich davon abhängig, welche technischen und organisatorischen Maßnahmen die betroffene Organisation in den Bereichen Prävention, Detektion und Reaktion getroffen hat: Selbst wenn Präventivmaßnahmen nicht gegriffen haben und den Vorfall nicht abwenden konnten, können wirkungsvolle Detektionsmaßnahmen sowie eine gute und schnelle Reaktion den Schaden für eine Organisation wirksam begrenzen.

Wie unterschiedlich die Schäden durch Ransomware sein können, zeigt auch die oben vorgestellte Umfrage des BSI zur Betroffenheit der deutschen Wirtschaft durch Ransomware:

Demnach waren bei ca. 70 Prozent der betroffenen Unternehmen nur einzelne Arbeitsplatzrechner von Ransomware befallen. Bei jedem fünften der betroffenen Unternehmen (22 Prozent) kam es zu einem erheblichen Ausfall von Teilen der IT-Infrastruktur und 11 Prozent der Betroffenen erlitten einen dauerhaften Verlust wichtiger Daten. 2 Prozent der Betroffenen gaben an, dass durch die Ransomware-Infektion die wirtschaftliche Existenz des Unternehmens bedroht ist oder war.
58 Prozent der Betroffenen gaben an, dass die Einschränkung durch die Ransomware-Infektion kurzfristig binnen 48 Stunden behoben werden konnte. Für 18 Prozent der betroffenen Unternehmen dauerte die Einschränkung länger als 48 Stunden.

Bei Ransomware-Infektionen werden Versäumnisse bei der Prävention und Wartung der IT deutlich:

- fehlende Sensibilisierung der Mitarbeiter und nicht umgesetzte technische Schutzmaßnahmen erhöhen die Wahrscheinlichkeit einer Ransomware-Infektion nach einer Spam-Welle
- fehlende Sicherheitsupdates und ein nicht zeitgerechtes Patch-Management erhöhen die Wahrscheinlichkeit einer Ransomware-Infektion durch Drive-By-Angriffe mit Exploit-Kits
- fehlende Netzsegmentierung, umfangreiche Freigaben und schwache Administrator-Passworte vergrößern die Zugriffsmöglichkeiten einer einzelnen Ransomware-Infektion und damit den Schaden für die gesamte Organisation
- fehlende, veraltete, unregelmäßige oder nicht überprüfte Daten-Backups machen die Wiederherstellung von Daten entweder unmöglich oder vergrößern den Zeitraum des Datenverlustes

2.8 Ausblick auf die Weiterentwicklung der Bedrohungslage

Aus der Perspektive der Cyber-Kriminalität sind die heutigen, breit gestreuten Angriffe mittels Ransomware ein Erfolgsmodell. Es ist zu erwarten, dass sich auch dieses Geschäftsmodell weiterentwickelt, um neue Opfer zu finden und zusätzliche Profite zu generieren. Dies kann sich z. B. darin zeigen, dass Cyber-Kriminelle zukünftig neben den Massenangriffen vermehrt gezielte bzw. manuell gesteuerte Angriffe auf ausgewählte Opfer durchführen mit dem Ziel, einen hohen Geldbetrag von der angegriffenen Organisation zu erpressen. In einem ersten Schritt wird dabei eine ausgewählte Organisation infiltriert, der Zugriff ausgeweitet und unternehmensrelevante Daten und Systeme sowie Backups identifiziert. Diese werden dann auf einen Angriff mittels Ransomware vorbereitet. Die Verschlüsselung aller Daten bzw. Systeme läuft zeitlich koordiniert ab. Durch weitere Maßnahmen, wie Störung der Kommunikation in der Organisation, können mögliche Mitigationsversuche verhindert und die Erfolgswahrscheinlichkeit weiter erhöht werden. Es ist davon auszugehen, dass sich mit dieser Art Angriff deutlich höhere Summen erpressen lassen als bei heutigen Angriffen mit Ransomware üblich.

Ist eine Organisation in dieser Form kompromittiert, ist es einzig von der Absicht der Täter abhängig, ob Daten kopiert (Spionage), Daten gelöscht (Sabotage) oder Daten verschlüsselt (Erpressung) werden.

3 Maßnahmen

Um Infektionen mit Ransomware zu verhindern oder einen eingetretenen Schaden zu minimieren, gibt es eine Vielzahl technischer und organisatorischer Maßnahmen in den Bereichen Prävention, Detektion und Reaktion. Viele dieser Maßnahmen sind keine neuen oder Ransomware-spezifischen Empfehlungen, sondern gehören zu den allgemeinen Best-Practices zur Verbesserung der IT-Sicherheit, dessen Umsetzung das BSI auch unabhängig von der aktuellen Gefährdungslage durch Ransomware empfiehlt. Die Zusammenstellung der Maßnahmen erfolgte jedoch speziell auf die aktuelle Bedrohungslage durch Ransomware.

3.1 Präventionsmaßnahmen

Im vorhergehenden Kapitel wurden die Angriffsvektoren beschrieben, die aktuell verwendet werden, um Systeme mit Ransomware zu infizieren. Um diesen Angriffen entgegenzuwirken oder die Auswirkungen einer Infektion zu minimieren, sollten die folgenden Präventionsmaßnahmen umgesetzt werden:

3.1.1 Maßnahmen gegen den Angriffsvektor Spam

Schutzmaßnahmen von Client-Systemen

Spam-E-Mails mit Schadprogrammen bzw. Droppern als Anhang und geschicktem Social Engineering sind aktuell einer der Haupt-Angriffsvektoren von Ransomware. Dementsprechend wichtig ist es, Maßnahmen gegen diesen Angriffsvektor umzusetzen, um die Schadenswirkung durch Ausführung von E-Mail-Anhängen oder heruntergeladenen Dateien zu reduzieren:

- Ausführung von Skript-Dateien wie JavaScript, VisualBasicScript oder PowerShell Scripts verhindern durch Maßnahmen wie:
  - Deaktivierung des Windows Script Hosts https://technet.microsoft.com/en-us/library/ee198684.aspx
  - Ausführung von VisualBasicScript einschränken https://technet.microsoft.com/en-us/library/ee198679.aspx
  - Deaktivierung von PowerShell mittels AppLocker bzw. Aktivierung der PowerShell-Protokollierung über die Gruppenrichtlinien. Es reicht nicht aus, die Skript-Ausführungsrichtlinie für Windows PowerShell auf Restricted zu setzen, da diese Einstellung über einen Parameter umgangen werden kann.
- Änderung der Standard-Dateizuordnung von Skript-Dateien, so dass diese nicht ausgeführt, sondern z.B. nur mit einem Texteditor (Notepad) angezeigt werden.
- Ausführung von Makros in Office-Dokumenten verhindern durch Maßnahmen wie:
  - Deaktivierung der Ausführung von Makros in Microsoft Office-Produkten https://technet.microsoft.com/de-de/library/ee857085.aspx#changevba
  - Aktivierung der geschützten Ansicht in Microsoft-Office-Produkten https://technet.microsoft.com/de-de/library/ee857087.aspx
    - Falls Geschäftsprozesse die Ausführung von Makros benötigen, kann deren Nutzung durch andere Einschränkungen und ergänzende Maßnahmen abgesichert werden:

    - Nutzung von vertrauenswürdigen Orten für Dokumente mit Makros https://support.office.com/en-us/article/Create-remove-or-change-a-trusted-location-for-your-files-f5151879-25ea-4998-80a5-4208b3540a62
    - Nutzung signierter Makros https://technet.microsoft.com/de-de/library/ee857085.aspx
    - Grundsätzlich sollte die Möglichkeit genutzt werden, innerhalb einer Organisation genutzte Makros digital zu signieren und deren Ausführung anhand festgelegter digitaler Signaturen zu erlauben.
- Einblenden von bekannten Datei-Erweiterungen im Windows-Explorer, damit die Nutzer die tatsächliche Dateiendung erkennen können und sich nicht nur auf die Korrektheit des Dateisymbols verlassen.

Schutzmaßnahmen auf Mail-Servern

Spam-Nachrichten sollten so früh wie möglich, also am besten bereits serverseitig, durch einen Spamfilter herausgefiltert werden.

Grundsätzlich sollte zudem erwogen werden, Dateien mit den nachfolgend genannten Dateipräfixen serverseitig zu blockieren oder die Bereitstellung via Quarantäne schrittweise zu regeln:

- Alle ausführbaren Dateiformate und Skripte, wie beispielsweise: .bat, .com, .chm, .cmd, .exe, .hta, .jar, .js, .jse, .lnk, .msi, .pif, .ps1, .scf, .scr, .ws, .wsf
- Verschlüsselte Archive / Zip-Dateien, wie zum Beispiel: .7z, .zip, .zipx, .rar
- Makro-Dateien (MIME/HTML-Kodierung betrachten): .bas, .vb, .vbs, .vbe
- Sollte eine Filterung für einzelne Dateitypen oder bestimmte Accounts nicht möglich sein, sollten potentiell gefährliche Anhänge enthaltende Spam-Nachrichten für den Nutzer gut sichtbar als "gefährlich" markiert werden.
- Weiterhin kann die Annahme von Spam-Nachrichten bereits am Mail-Server reduziert werden:
    - SPF (Sender-Policy-Framework) Implementierung auf dem SMTP-Server hilft dabei, die Annahme von nicht legitimen E-Mails zu reduzieren.
    - Mittels Greylisting kann die Zustellung von E-Mails durch die üblichen Spam-Bots effektiv verhindert werden.
    - Auch sollte der eigene E-Mail-Server die Annahme von E-Mails mit internem Absender (SMTP-Envelope und From-Header) von externen Quellen ablehnen (Anti-Spoofing Maßnahme).

Weitere Informationen und Empfehlungen des BSI:

- E-Mail-Sicherheit: Handlungsempfehlungen für Internet-Service-Provider v1.0 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_098.html

3.1.2 Maßnahmen gegen den Angriffsvektor Drive-by-Angriffe

Aktualisierung von Anwendungen und Patch-Management auf Client-Systemen

Die regelmäßige Aktualisierung von Anwendungen und die Etablierung eines Patch-Management-Prozesses ist eine Basismaßnahme der IT-Sicherheit, mit der Software-Schwachstellen geschlossen werden, die bei Drive-by-Angriffen auch zur Installation von Ransomware verwendet werden.

Sicherheitsupdates müssen unverzüglich nach deren Bereitstellung durch den jeweiligen Hersteller angewendet und im Unternehmensumfeld idealerweise über eine zentrale Softwareverteilung eingespielt werden. Besonders relevant sind dabei Anwendungen wie Webbrowser, Webbrowser-Plug-ins, E-Mail-Programme, PDF-Anwendungen oder Office-Programme, mit denen Inhalte aus dem Netzwerk oder Internet geöffnet oder betrachtet werden. Sicherheitslücken in diesen Anwendungen werden binnen kürzester Zeit für Cyber-Angriffe ausgenutzt.

Grundsätzlich gilt: je weniger Programme zum Öffnen von unbekannten Inhalten und zur Ausführung von unbekanntem Code zur Verfügung stehen, desto weniger Schwachstellen und Fehlkonfigurationen können durch einen Angreifer ausgenutzt werden. Daher sollte nicht benötigte Software generell deinstalliert werden.

Weitere Informationen und Empfehlungen des BSI:

- IT Grundschutz - B 1.14 Patch- und Änderungsmanagement
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01014.html
- Management von Schwachstellen und Sicherheitsupdates
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_093.html
- Der Warn- und Informationsdienst von CERT-Bund
  https://www.cert-bund.de/wid
- Die Schwachstellenampel von CERT-Bund
  https://www.cert-bund.de/schwachstellenampel
- Themenlagebild Drive-by-Exploits und Exploit-Kits (für Mitglieder der Allianz für Cyber-Sicherheit)
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/CUG/CUG1/Informationspool/CSLage/Themenlagebild/Drive-by-Exploits-und-Exploit-Kits/drive-by-exploits-und-exploit-kits.html

3.1.2.1 Sicherer Einsatz des Webbrowsers und Reduktion der Angriffsfläche

Das BSI empfiehlt die Verwendung eines Webbrowsers mit Sandbox-Technologie sowie einer schnellen Versorgung mit Sicherheitsupdates bei Bekanntwerden von Sicherheitslücken. Nicht zwingend benötigte Browser-Plug-ins (z. B. Adobe Flash, Oracle Java, Microsoft Silverlight) sollen entfernt oder deren Ausführung zumindest eingeschränkt werden (z. B. Click-to-Play oder Einschränken auf Seiten im Intranet). Darüber hinaus bieten die Hersteller der gängigen Browser integrierte Mechanismen zum Phishing- und Malware-Schutz.

Weitere Informationen und Empfehlungen des BSI:

- Sicherheitsmaßnahmen Webbrowser
  https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/Sicherheitsmassnahmen/sicherheitsmassnahmen_node.html
- Absicherungsmöglichkeiten beim Einsatz von Web-Browsern v1.0
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_047.html
- BSI-Empfehlung für sichere Web-Browser
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_071.html

3.1.3 Maßnahmen gegen weitere Angriffsvektoren

3.1.3.1 Absicherung der Remotezugänge sowie der von außen zugänglichen Systeme

Vereinzelt versuchen Angreifer, Ransomware über kompromittierte Remote-Zugänge auf Systemen oder Netzwerken zu installieren. In der Regel sollten diese immer über VPNs, zusammen mit einer Zwei-Faktor-Authentisierung, geschützt werden. Zusätzlich können eine Filterung nach Quell-IP-Adressen, ein Schutz gegen Brute-Force-Angriffe sowie ein Monitoring der exponierten Systeme die Absicherung unterstützen.

Andere Infektionen mit Ransomware sind auf Software-Schwachstellen in Servern (Webserver, Applikationsserver) zurückzuführen, die aus dem Internet erreichbar sind . Wie bei den Client-Systemen sind auch für diese exponierten Systeme Patch-Management-Prozesse zu etablieren und Software-Schwachstellen schnell zu schließen.

Aufgrund dieser Angriffsvektoren ist ein zuverlässiger Schutz der von außen erreichbaren Systeme und Dienste zwingend notwendig. Deren Exposition sollte in regelmäßigen Abständen in Form von Penetrationstest überprüft werden. Dabei werden die von extern erreichbaren Systeme identifiziert und auf ihre Anfälligkeit für Angriffe geprüft.

Weitere Informationen und Empfehlungen des BSI:

- Grundregeln zur Absicherung von Fernwartungszugängen v1.0
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_054.html
- Praxis-Leitfaden für IS-Penetrationstests
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/Leitfaden_IS_Pentest.html
- Sicheres Bereitstellen von Web-Angeboten (ISi-Web-Server)
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Web-Server/web_server_node.html
- IT-Grundschutz - B 5.4 Webserver
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05004.html
- Quartalsthema: Web Application Security
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Themen/WAS/web_application_security_content.html

3.1.4 Datensicherungskonzept und Backup

Ein regelmäßiges und funktionsfähiges Backup der Daten ist die wichtigste präventive Schutzmaßnahme, mit der auch im Falle einer Ransomware-Infektion die Verfügbarkeit der Daten und damit die Funktionsfähigkeit einer Organisation gewährleistet werden kann.

Jede Organisation sollte über ein Datensicherungskonzept verfügen und dieses auch umsetzen. Dazu gehören auch die Planung und Vorbereitung des Wiederanlaufs sowie der Rücksicherung der Daten. Datensicherungen müssen regelmäßig angefertigt, stichprobenartig auf ihre Funktion geprüft und unabhängig vom IT-Netz gelagert werden.

Die Notwendigkeit zur separaten Lagerung (Offline-Backup) resultiert insbesondere aus der Erfahrung, dass einige Ransomware-Familien nicht nur lokale Daten, sondern zusätzlich Daten auf Netzlaufwerken verschlüsseln. Ist ein Backup auf einem dauerhaft zugreifbaren Netzlaufwerk abgelegt, so kann auch das durch eine Ransomware-Infektion unbrauchbar gemacht werden.

Weitere Informationen und Empfehlungen des BSI:

- IT-Grundschutz: Entwicklung eines Datensicherungskonzepts https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m06/m06033.html

3.1.5 Einsatz von Virenschutzprogrammen

In großen Organisationen sollen Virenschutzprogramme für den Enterprise-Bereich zum Einsatz kommen, da diese mehr Konfigurationsmöglichkeiten sowie eine zentrale Administration und zentrales Logging ermöglichen. Unabhängig von Signaturupdates sollte auch immer die neueste Programmversion eingesetzt werden, da neue und verbesserte Erkennungsverfahren häufig nur in die aktuelle Programmversion integriert werden.

Neue Varianten von Schadsoftware werden nur selten sofort über normale Signaturen von Virenschutzprogrammen erkannt. Daher sollten konsequent alle verfügbaren Module der Schutzsoftware am Gateway als auch auf dem Client genutzt werden. Infektionen mit neuen Varianten können so durch die Intrusion Prevention (IPS)-Module, verhaltensbasierte Erkennungs-Module und Cloud-Dienste der Virenschutzprogramme verhindert werden. An Gateways sollten zusätzlich Black- / Whitelisting-Dienste genutzt werden, die Verbindungen zu verdächtigen URLs unterbinden.

Des Weiteren sollte beim Hersteller der Virenschutz-Lösung nach zusätzlichen Schutzmöglichkeiten und spezifischen Konfigurationsempfehlungen gegen Ransomware nachgefragt werden.

3.1.6 Mitarbeitersensibilisierung und Awareness

Die Sensibilisierung der Mitarbeiter für IT-Sicherheit ist essentiell, da viele Ransomware-Infektionen auf durch den Nutzer geöffnete E-Mail-Anhänge zurückzuführen sind. Bekannt sind viele erfolgreiche Varianten des Social Engineerings, in dem Angreifer eine persönliche Beziehung vortäuschen, Gewinne versprechen, mit günstigen Preisen locken, Fristen vorgeben oder auf anderem Weg das Interesse des Nutzer wecken und diesen zu Fehlhandlungen verführen.

In Awareness-Kampagnen und Schulungen für Anwender sollte ein gesundes Misstrauen gegenüber Informationen im Internet sowie der 'gesunde Menschenverstand' im Zusammenhang mit allen internetbasierten Kontakten gefördert werden. Zusätzlich sollte kontinuierlich über die zwei wesentlichsten Infektionsvektoren von Schadprogrammen informiert werden:

- Infektion durch Öffnen von Anhängen in E-Mails
- Drive-by-Angriffe bei Besuch kompromittierter Webseiten

E-Mails sollten vor dem Öffnen eines Anhangs immer gelesen und auf Echtheit überprüft werden. Es sollten auf keinen Fall Anhänge von E-Mails mit unbekanntem Absender oder zu nicht nachvollziehbaren Vorgängen geöffnet werden. Im Zweifel sollte die Echtheit einer Nachricht auf anderem Weg verifiziert und ein Anhang durch IT-Verantwortliche überprüft werden.

Anwender sollten auf Merkmale aktueller Angriffskampagnen hingewiesen werden, z.B. Art der E-Mails, Typ der Anhänge, Makros in Dokumenten (für Details siehe Kapitel 2), an denen ein Großteil gefährlicher E-Mails identifiziert werden können.

Zusätzlich sollte den Nutzern ein Ansprechpartner (z.B. der IT-Sicherheitsbeauftragte) zur Verfügung stehen, an den sie sich bei Unsicherheiten und Rückfragen wenden können, z.B. nachdem ein Anhang geöffnet wurde.

Oft enthalten E-Mails keine Anhänge, sondern Links zu weiterführenden Informationen im Internet, die durch einen Klick des Nutzers im Webbrowser geöffnet werden. Bei einem Drive-by-Angriff kann bereits der Besuch einer entsprechend manipulierten Webseite (Hinterlegung oder Weiterleitung auf eine Drive-by-Exploit) zu einer Ransomware-Infektion führen, ohne dass der Nutzer diese Infektion bemerkt. Wie bei Anhängen ist es auch hier notwendig, die Korrektheit von Links in E-Mails zu überprüfen und diese nicht unvermittelt aufzurufen.

Weitere Informationen und Empfehlungen des BSI:

- Drei Sekunden für mehr E-Mail-Sicherheit
  https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/3_Sekunden_E-Mail_Sicherheitscheck.html
- IT-Grundschutz G 5.42 Social Engineering
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05042.html
- Surfen Sie mit gesundem Menschenverstand
  https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Menschenverstand/menschenverstand_node.html

3.1.7 Weitere Maßnahmen zum Schutz vor oder zur Reduktion der Auswirkungen nach einer Ransomware-Infektion

Netzwerklaufwerke

Die Verschlüsselung von Daten durch aktuelle Ransomware-Familien ist nicht auf das lokale System beschränkt, sondern erfasst je nach Schadprogramm-Familie auch Dateien auf eingebundenen oder zugreifbaren Netzlaufwerken. Je unbeschränkter die Zugriffsmöglichkeiten eines Nutzers auf unterschiedliche und ggf. unternehmensweite Netzlaufwerke sind, desto größer sind auch die Auswirkungen nach einer Infektion mit Ransomware.

- Schreib-Zugriffe auf Netzlaufwerke müssen demnach segmentiert und die Rechtevergabe restriktiv nach dem Prinzip 'Need-to-know' vergeben werden.
- Nicht länger benötigte Rechte sollten dem Nutzer wieder entzogen werden, d.h. eine Rechteverwaltung sollte von regelmäßig bis hin zu situationsbedingter Bedürftigkeit überprüft werden.
- Netzlaufwerke müssen auch im Backup-Konzept berücksichtigt sein.
- Die Empfehlungen für Netzlaufwerke sollten in gleicher Form auch auf cloudbasierte Speicherdienste angewendet werden.

Weitere Informationen und Empfehlungen des BSI:

- IT-Grundschutz: Entwicklung eines Netzkonzeptes:
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02141.html

Sichere Administratorkonten

Grundsätzlich sollten mit privilegierten Konten nur Administratorentätigkeiten durchgeführt werden. Mit einem Administratorkonto sollten bspw. keine E-Mails gelesen oder auch nicht im Internet gesurft werden. Diese Tätigkeiten sollten nur mit normalen Nutzerrechten durchgeführt werden. Letztlich sollten Administratoren für ihre Tätigkeiten unterschiedliche Nutzerkonten mit den jeweils benötigten Privilegien nutzen.

Jedes System (insbesondere jeder Server und Client) sollte über ein einzigartiges lokales Administrationskennwort verfügen. Es gibt einige freie Tools, die die Verwaltung solcher lokalen Administratorenpasswörter in Domänen übernehmen können.

Privilegierte Konten können darüber hinaus immer zusätzlich durch eine Zwei-Faktor-Authentisierung geschützt werden.

Im Hinblick auf die Bedrohungslage durch Ransomware verhindert die Trennung von Benutzer- und Administratorkonten beispielsweise das in vielen Ransomware-Familien implementierte Löschen der Volumeschattenkopien, das standardmäßig nur mit administrativen Rechten möglich ist. Stehen nur normale Nutzerrechte zur Verfügung, können die Schattenkopien durch die Ransomware nicht gelöscht und ggf. zur Wiederherstellung der Nutzerdaten verwendet werden.
Auch das Überschreiben des Master Boot Records (MBR) der Ransomware Petya ist nur mit administrativen Rechten möglich.

Weitere Informationen und Empfehlungen des BSI:

- IT-Grundschutz: Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04309.html

Verhinderung unerwünschter Programmausführung

Ein Großteil aller Schadprogramm-Infektionen könnte verhindert werden, wenn die Ausführung unerwünschter Software grundsätzlich verhindert wird. Dazu existieren eine ganze Reihe an Maßnahmen. Die wichtigste dabei ist das sogenannte "Application Whitelisting". Diese lässt eine Ausführung nur von freigegeben Programmen zu.
Da die Verwaltung solcher Whitelists sehr aufwendig ist, kann stattdessen auch in einem ersten Schritt nur ein "Application Directory Whitelisting" eingesetzt werden. Dabei wird die Ausführung von Programmen nur aus bestimmten Verzeichnissen (z.B. C:\Windows, C:\Programme) erlaubt. Hierbei ist es wichtig, dem Nutzer die Schreibrechte auf diese Verzeichnisse zu entziehen, damit dieser, bzw. die Ransomware unter Verwendung seines Kontos, keine ausführbaren Dateien in diese Verzeichnisse kopieren kann. So würde zum Beispiel die Ausführung von Dateien im Verzeichnis %TEMP% unterbunden, wo Malware in der Regel beim Herunterladen abgelegt wird.

Durch entsprechende, einschränkende Konfiguration kann die Ausführung unerwünschter Schadprogramme, die zuvor durch einen E-Mail Schadanhang nachgeladen wurden, verhindert oder zumindest erschwert werden:

Weitere Maßnahmen, die die Ausführung unerwünschter Software verhindern können, sind:

- Kapselung / Entkopplung des Webbrowsers (ReCoBS / Terminal-Server, Virtuelle Maschine zum Surfen, ...).
- Microsoft Enhanced Mitigation Experience Toolkit
  Die Erfolgswahrscheinlichkeit von Angriffen kann durch Einsatz von EMET stark reduziert werden. EMET verhindert das Laden bestimmter Module durch geschützte Applikationen. Konkret wird einem Prozess das Laden bestimmter DLLs untersagt. Zum Beispiel wird verhindert, dass Microsoft Word das Adobe Flash Plug-in lädt.

Weitere Informationen und Empfehlungen des BSI:

- Anwendungsschutz vor ungepatchten Schwachstellen mittels EMET
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_040.html
- Sicherer Einsatz von Microsoft AppLocker v1.0
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_117.html
- IT-Grundschutz: M 4.419 Anwendungssteuerung ab Windows 7 mit AppLocker
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04419.html

Definition erlaubter Dateitypen auf Datei-Server

Der Ressourcen-Manager für den Microsoft Windows Datei-Server (File Server Ressource Manager) bietet die Funktion, eine Liste von Dateitypen zu definieren, die auf einem Datei-Server abgelegt werden dürfen. Damit ist es möglich, eine nicht gestattete Dateigruppe mit der Endung *.* zu erstellen und eine Liste mit Ausnahmen zuzulassen, die auf dem Dateiserver abgelegt werden dürfen (z. B. *.docx, *.xlsx, *.txt usw.). Somit wäre es mit einer entsprechenden Dateiprüfungsregel möglich, das Erstellen von Dateien mit anderen Endungen als die in der Liste der Ausnahmen aufgezählten zu verhindern. Durch die Möglichkeit der Protokollierung im Ereignisprotokoll können nicht genehmigte Schreibvorgänge erkannt und darauf reagiert werden.

Diese Maßnahme zum Schutz der Daten auf einem Datei-Server greift jedoch nicht bei Ransomware, die Dateien verschlüsselt, ohne dabei die Dateiendung zu ändern (z.B. TeslaCrypt ab Version 4).

Auf Linux Systemen ist eine ähnliche Alarmierung / Blockierung mit dem Paket Fail2Ban möglich. Dazu muss der Samba-Server so konfiguriert werden, dass alle Schreibvorgänge und Umbenennungen protokolliert werden. Anschließend wird Fail2Ban so konfiguriert, dass ein Alarm ausgelöst wird, wenn ein Nutzer zu viele Dateien auf einmal neu anlegt oder umbenennt. Gleichzeitig könnten diesem Nutzer auch die Schreibrechte entzogen werden, wodurch eine weitere Verschlüsselung gestoppt würde. Eine Konfigurationsanleitung findet sich unter
https://www.heise.de/security/artikel/Erpressungs-Trojaner-wie-Locky-aussperren-3120956.html.

Regelmäßige Schwachstellenscans und Penetrationstests

Als ergänzende Maßnahme können IT-Systeme mit einem Penetrationstest und regelmäßigen Schwachstellen-Scans darauf geprüft werden, ob die Härtungs- und Absicherungsmaßnahmen, beispielsweise gegen die Ausbreitung der Ransomware oder das Übergreifen auf Backup-Medien, geeignet umgesetzt worden sind. Bei solchen regelmäßigen Überprüfungen soll weiterhin überprüft werden, ob Aktualisierungen für Betriebssysteme, Webbrowser und andere Anwendungen laufend eingespielt werden.

Eine entsprechende Überprüfung kann auch durch einen externen Dienstleister durchgeführt werden. Auf den Webseiten der Allianz für Cyber-Sicherheit findet sich unter
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/zert_dienstleister/zertdienstleister.html eine Übersicht der durch das BSI zertifizierten IT-Sicherheitsdienstleister für IS-Revision und IS-Beratung sowie Penetrationstests.

Übungen

Kommt es in einer Organisation zu einer Schadprogramm-Infektion, ist eine schnelle Reaktion der Verantwortlichen notwendig, um

- die Auswirkungen der Infektion zu minimieren,
- die Infektion zu beseitigen und
- Neu-Infektionen sowie die Ausbreitungen des Schadprogramms zu verhindern.

Die dazu notwendigen Abläufe müssen definiert und regelmäßig geübt werden. Schon einfache Übungen können sensibilisieren und gleichzeitig überprüfen, wie eine Organisation in einem Vorfall reagieren würde. Damit werden außerdem auch Anforderungen aus dem Notfallmanagement, z.B. nach dem BSI Standard 100-4 oder allgemeiner aus dem Business Continuity Management (BCM), erfüllt.

Als Basis für die Überprüfung der Vorbereitung einer Organisation auf eine Ransomware-Infektion kann die Musterübung "Betroffen" mit geeigneten Anpassungen verwendet werden (verfügbar für Mitglieder der Allianz für Cyber-Sicherheit).

3.2 Detektionsmaßnahmen

3.2.1 Zentrale Sammlung und Auswertung von Logdaten

Wenn es zu einem Vorfall kommt, kann eine Auswertung von Logdaten dabei helfen, dessen Ausmaß festzustellen. Mit der Auswertung von zuvor erfassten Logdaten von Netzwerkkommunikation oder Systemereignissen können Infektionen des Netzwerks festgestellt, infizierte Systeme entdeckt und idealerweise der initiale Infektionsweg identifiziert werden.
Unternehmen sollten daher bereits im Vorfeld eine gut geplante und datenschutzkonforme Logging-Policy etabliert haben und sicherstellen, dass die Logs auch regelmäßig erzeugt und mittels zentraler Logserver sicher gespeichert werden. Dabei sollten auch Systemereignisse erfasst werden, die in Zusammenhang mit Ransomware-Infektionen stehen können, z.B. Protokollierung der Microsoft Windows PowerShell. Wird in einer Organisation bisher keine systematische Sammlung und Auswertung von Logdaten durchgeführt, sollte dies umgehend initiiert werden.

Weitere Informationen und Empfehlungen des BSI:

- IT-Grundschutz - B 5.22 Protokollierung
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05022.html
- IT-Grundschutz - M 2.500 Protokollierung von IT-Systemen
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02500.html?nn=6610622

3.2.2 Zugriffe am Netzübergang auf Kontrollserver überwachen und ggf. blocken

Die Überwachung der Zugriffe aus dem eigenen Netz auf bekannte Command & Control (C2) Server erlaubt eine Erkennung und Alarmierung, wenn kompromittierte Systeme auf diese Server zugreifen wollen. Anstatt die Kommunikation lediglich zu überwachen, kann diese auch direkt blockiert werden. Einige Ransomware-Familien benötigen eine Verbindung zu Steuerungs-Servern, bevor die Daten verschlüsselt

werden können. Sind diese Server-Adressen bekannt, kann die Verschlüsselung der Daten unterbunden werden.

Entsprechende Datenfeeds können bei IT-Sicherheitsdienstleistern eingekauft werden. Darüber hinaus bietet das Ransomware-Tracker Projekt von Abuse.ch Echtzeit-Informationen sowohl zu aktiven Ransomware C2-Servern als auch zu kompromittierten Seiten, die Nutzer mit Ransomware infizieren. Auch eine Zusammenstellung durch unterschiedliche Sicherheitsforscher zum Thema Ransomware unter https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/ ist eine gute Quelle für Indikatoren, die zur Detektion verschiedener Ransomware-Varianten genutzt werden können.

3.3 Reaktionsmaßnahmen

Wenn es trotz der oben beschriebenen Präventionsmaßnahmen zu einer Infektion mit Ransomware kommt, gilt es ruhig zu bleiben und bedacht zu handeln. Im Folgenden sind die aus BSI-Sicht wichtigsten Maßnahmen zusammengestellt, die als Reaktion auf eine Ransomware-Infektion zu ergreifen sind. Im Idealfall steht ein vorher definiertes und bereits erprobtes Notfallkonzept zur Verfügung, das nach der Entdeckung der Schadprogramm-Infektion abgearbeitet werden kann. Das BSI empfiehlt dazu die Umsetzung des BSI Standard 100-4 "Notfallmanagement".

Primäre Ziele der Reaktionsmaßnahmen bei einer Ransomware-Infektion sind

- die Begrenzung des eingetretenen Schadens bzw. die Verhinderung weiterer Schäden,
- die Identifikation und Isolation der betroffenen Systeme,
- das Finden und Schließen des Infektionsvektors, um eine erneute Infektion zu verhindern
- sowie die Rückkehr zu einem sicheren Normalbetrieb.

Entgegen der vom BSI empfohlenen Maßnahmen bei einem APT-Vorfall steht bei der Reaktion auf eine Ransomware-Infektion die wirkungsvolle Verhinderung weiterer Schäden im Vordergrund.

3.3.1 Incident Response

- Zur Begrenzung des bereits eingetretenen Schadens und zur Verhinderung weiterer Schäden sollten infizierte Systeme umgehend vom Netz getrennt werden. Dazu sollten Netzwerkkabel physisch vom infizierten System getrennt werden. Gleichermaßen sollten etwaige WLAN-Adapter entfernt oder deaktiviert werden, um betroffene Systeme zu isolieren.
- Ist die Ransomware nach der Entdeckung noch aktiv, kann die Verschlüsselung weiterer lokaler Daten durch das harte Ausschalten des Systems (Stromversorgung unterbrechen, Akku entfernen) unterbunden werden.

Durch ein abruptes Ausschalten eines infizierten Systems kann die Verschlüsselung sowie der Schlüsselaustausch in einem undefinierten Zustand verharren, wodurch eine Entschlüsselung nach Zahlung des Lösegeldes unmöglich wird.

Das BSI empfiehlt dennoch das Ausschalten des Systems, um weiteren Schaden zu verhindern und die verschlüsselten Daten aus einem Backup wiederherzustellen, anstatt auf eine ordnungsgemäße Entschlüsselung aller Daten nach Zahlung eines Lösegeldes zu hoffen.

- Zur Identifikation von betroffenen Systemen sollten Logdaten der Netzwerkverbindungen, der Client-Betriebssysteme sowie der zentralen Dienste analysiert werden. Eine Vielzahl von Schreibzugriffen von einem Client auf ein Netzlaufwerk kann ein Anhaltspunkt für eine Infektion sein.

Auch die Metadaten der verschlüsselten Dateien können Hinweise auf infizierte Systeme oder betroffene Nutzerkonten beinhalten. Auch Netzwerk-Verbindungen zu unbekannten Hosts oder IP-Adressen können Hinweise auf inzifierte Clients liefern.

- Besteht der Verdacht, dass mehrere Clients unabhängig voneinander infiziert, aber noch nicht identifiziert sind, können vorsorglich zentrale Dienste wie der Zugriff auf Datei-Server, Backup-Server oder die Internetkommunikation unterbunden werden.
- Über die Webseite https://id-ransomware.malwarehunterteam.com/ können anhand einer verschlüsselten Datei oder der abgelegten Erpressernachricht eine Vielzahl von Ransomware-Familie identifiziert werden. Ggf. steht für die Schadprogramm-Familie ein Tool zur Entschlüsselung zur Verfügung.
- Es muss sehr früh entschieden werden, ob eine forensische Untersuchung durchgeführt werden soll. Forensische Sicherungen von Zwischenspeicher und Festplatten sollten durch einen fachkundigen Mitarbeiter oder Dienstleister sinnvollerweise vor weiteren Reparaturversuchen oder Neustarts der betroffenen Systeme unternommen werden. Danach sind forensische Untersuchungen nur noch sehr schwer bzw. gar nicht mehr durchführbar. Vorhandene forensische Sicherungen können zusätzlich die Ermittlungsarbeit der Polizei unterstützen.

- Konnte der Angriffsvektor der Ransomware-Infektion identifiziert werden, ist die Umsetzung der empfohlenen Präventionsmaßnahmen sicherzustellen, um Neuinfektionen zu verhindern.

Weitere Informationen und Empfehlungen des BSI:

- Leitfaden IT-Forensik
  https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/IT-Forensik/forensik_node.html

3.3.2 Externe Expertise

Falls betroffene Organisationen kein eigenes IT-Security oder Computer Emergency Response Team (CERT) haben, welches den Vorfall bewältigen kann, empfiehlt das BSI externe Unterstützung durch Spezialisten einzukaufen. Auf den Webseiten der Allianz für Cyber-Sicherheit finden Sie eine Übersicht über durch das BSI zertifizierte IT-Sicherheitsdienstleister für IS-Revision und IS-Beratung sowie Penetrationstests.

3.3.3 Wiederherstellung der Daten

Bevor mit der Datenwiederherstellung begonnen wird, ist eine Neuinstallation des infizierten Systems erforderlich. Das verwendete Betriebssystem sollte von einem vertrauenswürdigen Datenträger stammen. Ebenso sollte das Backup auf Schadprogramme überprüft werden, um eine sofortige Neuinfektion zu verhindern.

Unter bestimmten Voraussetzungen ist auch ohne Datensicherung eine teilweise oder komplette Wiederherstellung der Daten möglich, z.B. wenn

- die Ransomware Schattenkopien in Windows nicht gelöscht hat,
- Snapshots von virtuellen Maschinen und deren Daten existieren,
- frühere Dateiversionen bei Netzlaufwerken oder Cloud-Diensten existieren,
- die forensische Wiederherstellung gelöschter Dateien möglich ist.

Eine Entschlüsselung kann unter Umständen auch funktionieren, wenn Entschlüsselungs-Tools für die betreffende Ransomware-Familie zur Verfügung stehen. Eine Auflistung von Entschlüsselungsprogrammen

aktueller Ransomware-Familien findet sich in Kapitel 1. Steht kein Backup zur Wiederherstellung der Daten zur Verfügung, können vor der Neuinstallation des Systems die verschlüsselten Daten gesichert werden, falls in Zukunft ein Entschlüsselungs-Tool für die betreffende Ransomware-Familie zur Verfügung steht.

Auf die Möglichkeiten einer Datenwiederherstellung ohne Backup sollte man sich jedoch nicht verlassen. Ein aktuelles und funktionierendes Backup ist daher Grundvoraussetzung für eine wirksame und schnelle Wiederherstellung der Daten.

3.3.4 Lösegeld

Bei Ransomware handelt es sich um eine digitale Form der Lösegelderpressung durch die Organisierte Kriminalität.

Das BSI empfiehlt allen Betroffenen, nicht auf die Forderungen einzugehen und kein Lösegeld zu zahlen.

Stattdessen sollte die Ransomware-Infektion wie zuvor beschrieben beseitigt und die betroffenen Daten aus einer Datensicherung wiederhergestellt werden.

Es gibt keine Garantie, dass nach Zahlung eines Lösegeldes ein Schlüssel oder ein funktionsfähiges Programm zur Verfügung gestellt wird, das eine Entschlüsselung ermöglicht. Stattdessen belegt jede erfolgreiche Erpressung den Erfolg der Angriffsmethode und motiviert den Angreifer zu weiteren Straftaten. Lösegeldzahlungen finanzieren somit direkt die Weiterentwicklung der Schadsoftware und fördern deren Verbreitung. Zusätzlich steigt mit jedem gezahlten Lösegeld die Wahrscheinlichkeit für den Betroffenen, erneut Opfer einer Erpressung zu werden, vielleicht sogar über zielgerichtete Verfahren.

3.3.5 Anzeige erstatten

Das BSI empfiehlt betroffenen Organisationen darüber hinaus eine Strafanzeige zu erstatten, um das Geschäftsmodell durch den Fahndungsdruck polizeilicher Ermittlungen zu stören und einzudämmen.

Die Bundesländer bzw. die zuständigen Landeskriminalämter haben Anlaufstellen eingerichtet, die Unternehmen, welche Opfer von Cyber-Straftaten geworden sind, beratend zur Seite stehen und bei einer Anzeige unterstützen. Eine Liste der Anlaufstellen sowie eine Broschüre zum Thema sind auf den Webseiten der Allianz für Cybersicherheit unter
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/ZAC/polizeikontakt.html zu finden.

Privatpersonen können bei der nächsten lokalen Polizeidienststelle Anzeige erstatten.

4 Weitere Informationen

4.1 Pressemitteilungen und Kurzmeldungen des BSI sowie Beiträge der BSI-Mediathek zum Thema Ransomware

27.04.2016: Ransomware: Ein Drittel der Unternehmen ist betroffen

15.04.2016: Ransomware: Hoffnung für Petya-Geschädigte

13.04.2016: BSI startet Umfrage zur Ransomware-Betroffenheit

03.04.2016: Virus "Locky": Erpresser-Trojaner verbreitet sich rasant in Deutschland

23.03.2016: Cyberattacken auf Krankenhäuser

11.03.2016: BSI veröffentlicht Themenpapier zu Ransomware

08.03.2016: IT-Sicherheitsvorfälle beeinträchtigen Funktionsfähigkeit Kritischer Infrastrukturen

05.03.2016: Erpressungs-Trojaner: Daten als Geiseln

29.02.2016: n-tv Beitrag Computervirus Locky mit O-Ton Arne Schönbohm

29.02.2016: n-tv Interview mit BSI-Präsident Arne Schönbohm zum Thema Computersicherheit

22.02.2016: Krypto-Trojaner: Backups schützen gegen Datenverlust

05.02.2016: Safer Internet Day: BSI informiert über Risiken durch Ransomware

4.2 Allianz für Cyber-Sicherheit

Die Allianz für Cyber-Sicherheit ist eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) gegründet wurde.

Als Zusammenschluss aller wichtigen Akteure im Bereich der Cyber-Sicherheit in Deutschland hat die Allianz das Ziel, aktuelle und valide Informationen zu Gefährdungen im Cyber-Raum bereitzustellen.

Im Informationspool der Allianz für Cyber-Sicherheit finden Sie aktuelle Inhalte zu gegenwärtigen Cyber-Bedrohungen - verfasst vom Bundesamt für Sicherheit in der Informationstechnik und den Partnern der Allianz für Cyber-Sicherheit. Mit diesen Inhalten können Sie Ihre Schutzmaßnahmen stets an die momentane Bedrohungslage anpassen.

Dazu gehören unter anderem:

- BSI Cyber-Sicherheits Warnmeldungen
- BSI Cyber-Sicherheits Vorfallsinformation
- BSI Themenlagebilder
- BSI Musterübungen

Jedes Unternehmen bzw. jede Institution in Deutschland kann über eine kostenlose Mitgliedschaft in der Allianz für Cyber-Sicherheit Zugriff auf den Informationspool erhalten.