Bundesamt
für Sicherheit in der
Informationstechnik

Ransomware

Bedrohungslage, Prävention & Reaktion

Nationales IT-Lagezentrum
Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: bsi@.bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einführung

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und eine Freigabe dieser Ressourcen erfolgt nur gegen Zahlung eines Lösegeldes (engl. ransom). Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.

Seit Mitte September 2015 hat sich die Bedrohungslage durch Ransomware deutlich verschärft. Es treten vermehrt Fälle auf, über einige wurde auch öffentlich berichtet. Weil der Leidensdruck für die Betroffenen so hoch ist, zahlen Opfer in vielen Fällen das geforderte Lösegeld. Dieser Erfolg der Täter führt dazu, dass mittlerweile Kapazitäten aus dem "Banking-Trojaner-Geschäft" abgezogen werden und die Botnetze nun Ransomware verteilen.

Bereits seit 2010 / 2011 wird Ransomware verbreitet für Cyber-Angriffe eingesetzt. Auch davor gab es bereits erste Varianten dieses Schadprogramm-Typs. Einfache Ransomware-Varianten zeigen z. B. einen Sperrbildschirm an und hindern die Anwender an der Nutzung ihres Systems. Über eindringliche Warnungen und Aufforderungen wurde behauptet, dass das System im Zuge polizeilicher oder sonstiger staatlicher Ermittlungen (BKA, BSI, international FBI, CIA ...) gesperrt sei und nur gegen Zahlung eines Bußgeldes oder Strafzahlung wieder freigegeben wird.

Im Zuge der Weiterentwicklung werden vermehrt Ransomware-Varianten entwickelt, die Daten auch verschlüsseln, welche dann dauerhaft (auch nach Bereinigung des Schadprogramms) nicht mehr zur Verfügung stehen. Für die Verschlüsselung werden als sicher anzusehende Algorithmen eingesetzt, somit ist eine Entschlüsselung nicht möglich. Zusätzlich zu den Daten des infizierten Clients werden auch Daten auf zugänglichen Netzlaufwerken oder eingebundenen Cloud-Diensten verschlüsselt.

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 anonymen Guthaben- und Bezahlkarten kommt. Im Vergleich zu Cyber-Angriffen über Banking-Trojaner sind weder Mittelsmänner für Überweisungen noch Waren-Agenten notwendig, um einen erfolgreichen Angriff zu monetarisieren.

Für das Opfer ist der wesentliche Unterschied gegenüber einer Betroffenheit mit klassischen Schadsoftware wie Banking-Trojanern, DDoS-Tools, Zugangsdaten- und Identitäts-Phishern, dass der Schaden unmittelbar eintritt und ganz konkrete Konsequenzen für den Betroffenen hat. Hier verhindert oder erstattet keine Bank den Schaden, oder der PC funktioniert nur "etwas langsamer" weil im Hintergrund Dritte angegriffen werden, stattdessen sind zum Beispiel die Kinderbilder und alle Kontakte verloren oder die Unternehmensdaten nicht mehr zugreifbar oder kritische Dienstleistungen nicht mehr verfügbar. Es helfen meist nur präventive Maßnahmen und vor allem Backups.

Dieses Dokument stellt neben einer kurzen Darstellung der Bedrohungslage konkrete Hilfen für die Prävention und die Reaktion im Schadensfall bereit.

2 Bedrohungslage

Ransomware ist ein für Cyber-Kriminelle ein seit Jahren etabliertes Geschäftsmodell und betrifft Desktop-Betriebssysteme wie Microsoft Windows und Apple Mac OS, Server-Systeme unter Linux als auch mobile Betriebssysteme wie Google Android.
Infektionsvektoren von Ransomware für Desktop-Systeme sind aktuell hauptsächlich E-Mail-Anhänge oder Drive-By-Angriffe mittels Exploit-Kits.

Seit Dezember 2015 beobachtet das BSI große Spam-Wellen, über die massenhaft Ransomware verteilt wird. Dazu wird unter anderem die Infrastruktur des Dridex-Botnetzes verwendet, mittels der vorher Banking-Trojaner verteilt wurden. Daneben gibt es auch vermehrt Meldungen über Infektion mit Drive-By-Exploits auf infizierten Webseiten und Werbebannern.

Die Auswirkungen der Spam-Wellen lassen sich auch anhand dem BSI vorliegenden Detektionszahlen für Deutschland nachvollziehen. Gegenüber Oktober 2015 wurden im Februar 2016 mehr als 10-mal so häufig Ransomware durch Virenschutzprogramme in Deutschland detektiert. Aber auch weltweit stieg die Anzahl der Detektionen um den Faktor 6 an.

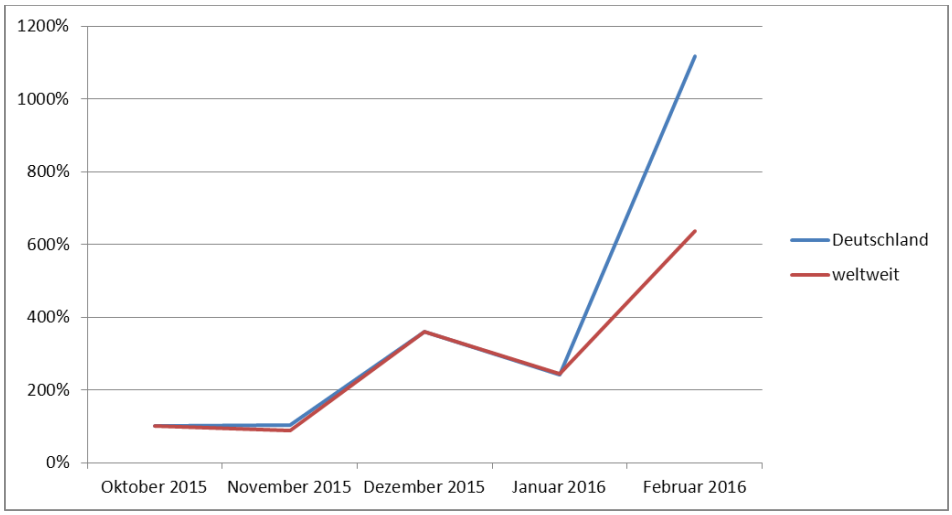

Abbildung 1: Trend der Ransomware-Detektionen in Deutschland Oktober 2015 – Februar 2016, Quelle: BSI

Die folgenden Punkte zeigen, warum sich das Geschäftsmodell für die Angreifer rentiert:

- Hoher Leidensdruck beim Opfer
- Bei Geschädigten sind ggf. die Wiederherstellungsaufwände größer als die Erpressersumme.
- Zahlung in Bitcoins sind anonym und sofort realisierbar. Sie müssen nicht aufwändig über Geldboten/Moneymules und Warenagenten gewaschen werden.

Angriffsvektoren

Im Folgenden werden die gebräuchlichsten Angriffsvektoren für Ransomware beschrieben.

2.1.1 Spam

Bei Angriffen mittels Spam wird versucht, über meist professionelles Social Engineering den Benutzer zum Öffnen von E-Mail-Anhängen zu bewegen. So werden angebliche Rechnungen, Bestellbestätigungen, Paketempfangsbestätigungen, eingescannte Dokumente, empfangene Faxe, teilweise unter Verwendung von

echten Firmennamen und -adressen und zum Teil in perfekter Nachahmung tatsächlicher Firmen-E-Mails, versendet. Im Anhang befindet sich meist ein sog. Downloader, der die eigentliche Schadsoftware nachlädt. So bleibt das Verteilungsnetz flexibel, da die Angreifer die zum Download bereit gestellte Schadsoftware auf aktuellem Stand (d. h. schlechte AV-Erkennung) halten können. Der Download findet meist von kompromittierten Webservern vor allem kleiner Webpräsenzen statt. Es wird vermutet, dass die Angreifer diese Webpräsenzen über Schwachstellen in nicht aktuell gehaltener Serversoftware und über Trojaner abgegriffene Zugangsdaten die Webserver kompromittieren konnten. In der Vergangenheit wurden auch Kampagnen gesichtet, in denen die Schadsoftware direkt verteilt wurde, z. B. als (meist gezippte) EXE-Datei oder eingebettet / kodiert in einem Microsoft-Office-Dokument. Das Entpacken und Starten musste dann vom Benutzer manuell durchgeführt werden oder wurde von Makros erledigt.

In den bisher am weitesten verbreiteten Kampagnen wurden Microsoft Office Dokumente mit stark verschleierten Makros (teilweise mit ungewöhnlichen Kodierungen wie HTML oder MIME) und JavaScript- sowie VirtualBasicScript-Dateien versendet. Oft wurden die Dateien in einem Archiv (meist ZIP) ausgeliefert.

Unter anderem wurde das auf die Verteilung des Banking-Trojaners DRIDEX spezialisierte Spamnetzwerk, die seit Monaten größte Schadsoftware-Spam-Quelle, Mitte Februar auf Verteilung der Ransomware LOCKY umgestellt. Als Größenordnung kann man Erfahrungen aus dem DRIDEX-Vorläufer GEODO extrapolieren, bei dem auf einem von vielen Kommando-Servern (C&C) binnen eines Monats etwa 60.000 deutsche Betroffene verwaltet wurden.

Der Versand der DRIDEX/LOCKY-Downloader erfolgt meist aus Schwellen- und Entwicklungsländern, wahrscheinlich, weil dort die Infektionen nicht so gut mittels Bankingbetrug bzw. Ransomware monetarisiert werden können.

2.1.2 Drive-By Infektionen mittels Exploit-Kits

Exploit-Kits gehören seit mehreren Jahren ebenfalls zu den Infektionsvektoren für Ransomware. Zero-Day-Exploits oder Exploits für neue Schwachstellen in weit verbreiteten Programmen werden binnen kürzester Zeit in Exploit-Kits integriert und auch zur Verteilung von Ransomware oder anderen Schadprogramm-Typen verwendet. In den vergangenen Monaten ging von den Exploit-Kits

- Angler
- Neutrino
- Nuclear
- Magnitude
- Rig

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

In vielen Fällen werden die Exploit-Kits über Drive-By-Infektionen auf kompromittierten Webseiten oder Werbebannern verbreitet. Danach wird die jeweilige Schadsoftware, z. B. Ransomware, nachgeladen.

2.1.3 Schwachstellen in Servern

Die Ransomware CTB-Locker nutzt Schwachstellen in Webservern zur Infektion aus und verschlüsselt dann die Inhalte des Web-Auftritts.

2.1.4 Ungeschützte Fernwartungszugänge

Bei Vorfällen mit der Ransomware GPCode wurde in einigen Fällen ein zusätzlicher Modus Operandi der Täter festgestellt. Diese scannen das Internet aktiv nach solchen Systemen, die Fernwartungszugänge ins Internet anbieten, wie zum Beispiel Microsoft Remote-Desktop. Dort führen Sie Brute-Force Angriffe auf das Passwort durch. Bei einem erfolgreichen Login installieren sie eine Ransomware-Malware.

Aufgrund der geringen Verbreitung von GPCode wird dieser Infektionsvektor durch Ransomware aber nur selten ausgenutzt.

2.2 Ransomware Varianten

Nach Erkenntnissen des BSI wurden im Februar 2016 in Deutschland am häufigsten die Ransomware-Familien TeslaCrypt, Locky sowie CryptoWall detektiert. Die Detektionszahlen zeigen auch, dass es sich bei 95 % der Angriffe um Ransomware mit Verschlüsselungsfunktion handelt. Die einfachen Sperrbildschirme im Desktop-Bereich aus den vergangenen Jahren haben heute keine Relevanz mehr.

Die Zahlen werden durch das Ransomwaretracker-Projekt von Abuse.ch bestätigt. Nach der aktuellen Statistik von abuse.ch führt TeslaCrypt unter der Anzahl der analysierten Ransomware Samples deutlich.

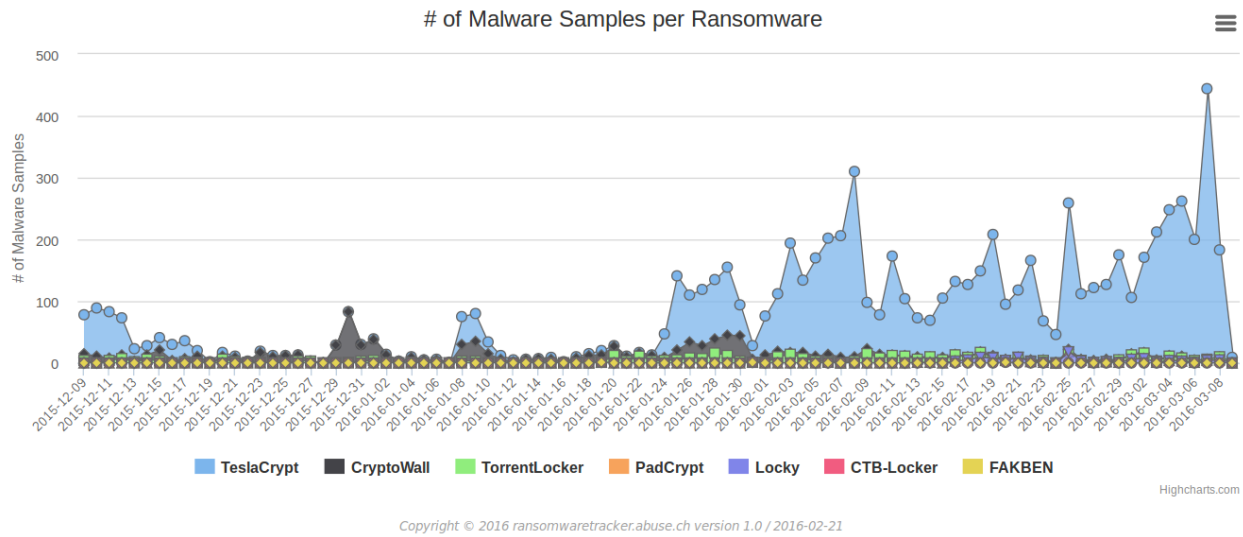

Abbildung 2: Vom Abuse.ch verarbeitete Ransomware-Samples pro Tag, Dezember 2015 – März 2016, Quelle: Ransomwaretracker.abuse.ch

2.3 Lage in den Unternehmen

Bei Ransomware-Vorfällen werden Versäumnisse bei der Prävention deutlich aufgezeigt. Schlecht gepflegte Systeme, fehlende, veraltete oder nicht überprüfte Software-Backups, schwache Administrator-Passworte, fehlende Netzsegmentierung uvam. rächen sich bei Ransomware sofort durch die eingetretenen Schäden.

Auch das Verhalten der Mitarbeiter spielt eine zentrale Rolle. Einige Angriffe sind mittlerweile so gut, dass sie kaum oder schwer zu erkennen sind. Dabei sind viele der beobachteten Ransomware-Spamwellen nicht mit großem Aufwand gestaltet. Hier würde eine Sensibilisierung der Mitarbeiter helfen.

Anzeichen für Banking-Trojaner und DDoS-Angriffsclients werden auf den Clients teilweise ignoriert bzw. nicht aktiv verfolgt. Genauso werden häufig Fehlkonfigurationen von Systemen vernachlässigt, da diese keine Auswirkung auf den Wirkbetrieb haben. Die Schäden im Unternehmen sind in diesen Fällen nur gering. Die Schutzgelderpressung führt nun zu konkreten Schäden, bei denen man nicht mehr "wegschauen" kann.

Bei Ransomware muss aktiv mit dem Ausfall von Dienstleistungen umgegangen werden (Näheres dazu siehe im Abschnitt "Potentielle Schäden"). Hier kann der Sicherheitsvorfall nicht mehr lokal gehalten oder klein geredet werden. So werden Häufungen von Vorfällen in bestimmten Branchen von den Medien bereitwillig

aufgegriffen, kommentiert und diskutiert - wobei die öffentlich verfügbare bzw. gesicherte Faktenlage in der Regel so dünn ist, dass bei der Berichterstattung oft spekuliert wird. Die Berichterstattung über Vorfälle in diversen deutschen Krankenhäusern zeichnet z. B. das Bild einer äußerst verletzbaren Branche. Im Austausch zwischen den IT-Verantwortlichen verschiedener Krankenhäuser und dem BSI zeigt sich hingegen, dass Angriffsversuche mit Ransomware (und Angriffe per E-Mail-Anhang und Fake-URLs) für viele Häuser zum normalen Tagesgeschäft gehören und durch Standardschutzmaßnahmen vereitelt werden.

2.4 Potentielle Schäden

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 mit 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 länger 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 weiterhin 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 neu in Werbung, Kundenbindung und Image 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 Material-Abnahmen 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 oben genannten Kategorien zur Folge haben.

Das Schadensausmaß ist erheblich davon abhängig, wie die betroffenen Organisation technisch und organisatorisch vorbereitet ist: Selbst wenn Präventivmaßnahmen nicht gegriffen haben und die Störung nicht abwenden konnten, kann eine gute Bewältigungsstrategie den Schaden erheblich begrenzen. Eine aktuelle Umfrage in der Branche hat dies noch einmal ausdrücklich bestätigt: Das Schadensausmaß reichte demnach von "Wir konnten die Verursacher innerhalb kurzer Zeit identifizieren und abschalten." über "Nach 4 Stunden waren die betroffenen Datenbestände wiederhergestellt und es konnte normal weitergehen." bis hin zu "Wir konnten 1 Woche lang nur die Notfallversorgung anbieten.".

Aus der Umfrage lassen sich u. a. folgende entscheidende Einflussfaktoren für das Schadensausmaß ableiten:

1. Wie schnell ist die Organisation in der Lage, die Störung überhaupt als solche zu identifizieren? Für den Anwender äußert sich die Aktivität einer Ransomware oftmals zunächst nur darin, dass er auf Dateien bzw. Informationen keinen Zugriff mehr erhält. Die Ursache (= Verschlüsselung) ist (in der Regel) nicht sofort ersichtlich. Erst wenn sich entsprechende Anwenderbeschwerden beim IT-Support "häufen", kann dort der Hinweis auf ein "größeres Problem" wahrgenommen werden. Je

eher der IT-Support die Warnsignale erkennt (und je besser er über mögliche Anzeichen informiert ist), desto eher kann er die Suche nach den Verursacher-Geräten in Gang setzen.

2. Wie schnell (und sicher) kann die Organisation die Geräte identifizieren, von denen aus die Ransomware die Verschlüsselung durchführt?
   Je eher die Verursacher gefunden sind, desto schneller können sie abgeschaltet und der Verschlüsselungsvorgang unterbrochen / abgebrochen werden. Eine wichtige Voraussetzung für ein schnelles Auffinden der infizierten Geräte ist die aktuelle Übersicht über (möglichst) alle in der Infrastruktur befindlichen Geräte. In komplexen (weil z. B. gerätetechnisch heterogenen) Infrastrukturen ist dies oft eine große Herausforderung.
   Kann das IT-Team sicherstellen, dass alle infizierten Geräte identifiziert wurden, kann mit dem Abschalten bzw. Isolieren dieser Geräte auch sichergestellt werden, dass die Gefahr gebannt ist.
3. Wie alt ist sind die jüngsten, vollständigen und intakten Backups?
   Können die infizierten Geräte abgeschaltet oder isoliert werden, kann mit dem "Aufräumen", also dem Neuaufsetzen der beschädigten (Fileserver-)Systeme und dem Rücksichern der Daten begonnen werden. Dabei liefern Snapshots bzw. Backup-to-Disk zwar die beste Aktualität, jedoch auch das Risiko, dass sie selbst der Verschlüsselung zum Opfer gefallen sind (womit wieder auf ältere Snapshots zurückgegriffen werden müsste).
4. Ist das Wiedereinspielen / die Rücksicherung vorbereitet und geübt?
   In einigen Fällen entstanden bei Wiedereinspielen der Backups durch die komplexen Abhängigkeiten und die z. B. Virtualisierung komplexer Systeme weitere Störungen und Ausfälle, die die Wiederinbetriebnahme der Systeme weiter verzögerten.
5. Welche Geräte sind von der Verschlüsselung betroffen?
   Je länger die Ransomware aktiv war und je mehr Datenbestände ihr zum Opfer fielen, desto größer ist die Gefahr, dass betriebsnotwendige Geräte ihre Arbeit nicht mehr verrichten können - entweder, weil ihre lokalen Datenbasis beschädigt wurde, oder ihre zentral gehaltene Datenbasis. Wenn, beispielsweise durch Netzwerksegmentierung oder durch restriktive Zugriffsbeschränkungen, verhindert werden konnte, dass betriebsnotwendige Daten der Nutzbarkeit entzogen wurden, kann der reguläre Geschäftsbetrieb (zumindest zum größten Teil) ungestört weiterlaufen. Im Negativfall ist entscheidend, wie schnell die zerstörten Datenbestände und die Funktionsfähigkeit der betroffenen Geräte wiederhergestellt werden können und wie aktuell die wiederhergestellten Daten sind. Dann ist mit einem temporären Ausfall wichtiger Geschäftsprozesse zu rechnen und mit einer zusätzlichen Arbeitsbelastung um die Datenbestände wieder á jour zu bekommen.

3 Vorbemerkung für die folgenden Maßnahmen

Die im Folgenden dargestellten präventiven und reaktiven Maßnahmen stellen nur einen kleinen Teil der möglichen Maßnahmen dar. Umfangreiche Beschreibungen finden Sie in den zahlreichen Veröffentlichungen des BSI. Insbesondere sei hier auf das Konzept IT-Grundschutz[1] verwiesen.

Die folgende Sammlung wurde speziell unter dem Blickwinkel Ransomware zusammengestellt. Es schützen und helfen die Maßnahmen auch bei anderen Angriffsarten.

1 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

4 Präventionsmaßnahmen

In diesem Kapitel werden Maßnahmen beschrieben, die eine Infektion mit Ransomware verhindern oder auch das Schadensausmaß begrenzen können.

4.1 Infektion verhindern

Im vorhergehenden Kapitel wurden die Angriffsvektoren beschrieben, die von Ransomware genutzt werden. Es werden im folgenden Maßnahmen vorgestellt, die eine Infektion über diese Angriffsvektoren verhindern können.

4.1.1 Patches

Um generell vor Infektionen durch die Ausnutzung bereits behobener Sicherheitslücken geschützt zu sein, sollten Updates und Patches unverzüglich nach der Bereitstellung durch den jeweiligen Softwarehersteller auch in die IT-Systeme - idealerweise über zentrale Softwareverteilung - eingespielt werden.

Die größte Gefahr besteht hierbei in der Regel für Anwendungen, mit denen Inhalte aus dem Netzwerk/Internet geöffnet werden, wie z. B. Web-Browser, Browser-Plugins, E-Mail-Programme, PDF-Dokumentenbetrachter und Office-Suiten.

4.1.2 Angriffsfläche minimieren

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. In Web-Browsern sollten insbesondere die Ausführung aktiver Inhalte zumindest eingeschränkt (z. B. Click-to-Play oder Einschränken auf Intranetseiten) sowie nicht zwingend benötigte Browser-Plugins (z. B. Flash, Java, Silverlight) entfernt werden.

Da teilweise Ransomware als E-Mail-Anhang in Form von Javascript und VisualBasic-Skripten verteilt wurde, sollte geprüft werden, ob auf die Ausführung von Skripten im Betriebssystem gänzlich verzichtet werden kann. Die Deaktivierung im Betriebssystem verhindert in diesem Fall eine Infektion, da der schadhafte Anhang nicht mehr versehentlich (z. B. durch einen Doppelklick) ausgeführt werden kann.

4.1.3 Behandlung von E-Mails / Spam auf dem Client

Viele E-Mails werden heutzutage als sogenannte HTML-E-Mails versendet. Damit diese im E-Mail-Programm korrekt dargestellt werden können, nutzt der E-Mail-Client jedoch die gleichen Mechanismen zur Darstellung wie der Web-Browser. Aufgrund der Größe der Darstellungskomponenten und der Vielzahl an Funktionen, enthalten diese jedoch häufig Schwachstellen, welche bei Web-Browsern durch zusätzliche Sicherheitsmaßnahmen eingedämmt werden. Dieser umgebende Schutz ist bei E-Mail-Programmen in der Regel weniger ausgeprägt. Die größte Schutzwirkung bietet in diesem Fall die Darstellung von E-Mails als Textdarstellung (oft als "Nur-Text" bzw. "reiner Text" bezeichnet im Gegensatz zur Darstellung als "HTML-Mail"). Ein weiterer sicherheitstechnischer Vorteil dieser Darstellung ist, dass Webadressen in der Textdarstellung nicht mehr verschleiert werden können (In einer HTML-E-Mail könnte ein Link mit der Bezeichnung "www.bsi.de" z. B. in Wahrheit auf die Adresse "www.schadsoftwaredownload.de" verweisen). Mindestens sollte die Ausführung aktiver Inhalte bei Verwendung von HTML-Mails unterdrückt werden. Somit würden entsprechende, schadhafte Skripte (vergl. "Angriffsfläche minimieren") nicht mehr ausgeführt werden können.

Folgende Einstellung sollten für den Umgang mit MS-Office-Dokumenten-Makros (MIME/HTML-Kodierung betrachten) auf dem Client konfiguriert werden:

- JS/VBS: automatisches Ausführen bei Doppelklick verhindern
- Makros im Client (per Gruppenrichtlinie) deaktivieren
- Vertrauenswürdige Orte für Makros im AD konfigurieren
- Signierte Makros verwenden

Grundsätzlich sollten Makros, die in einer Institution genutzt werden, digital signiert sein und nur die Ausführung von Makros mit festgelegten digitalen Signaturen erlaubt werden.

Auch kann man durch eine entsprechende Konfiguration das Nachladen der Ransomware durch einen Dropper in einer E-Mail verhindern oder zumindest erschweren:

- Ausführung von Programmen (per Gruppenrichtlinie) nur aus nicht durch den Benutzer beschreibbaren Verzeichnissen (Execution Directory Whitelisting), was die effektivste Maßnahme zum Schutz vor Malware darstellt
- Entkopplung von Browser und APC (ReCoBS / Terminal-Server, Surf-VM, ...

4.1.4 Behandlung von E-Mails / Spam auf dem Server

Spam sollte bereits durch einen Spamfilter serverseitig gefiltert oder mindestens markiert werden.

Grundsätzlich sollten folgende Dateien blockiert oder zumindest in Quarantäne verschoben werden:

- Alle ausführbaren Anhänge, auch wenn diese in Archiven enthalten sind. Beispiele (nicht abschließend): .exe, .scr, .chm, .bat, .com, .msi, .jar, .cmd, .hta, .pif, .scf
- Verschlüsselte Archive / Zip-Dateien.
- MS-Office-Dokument-Makros (MIME/HTML-Kodierung betrachten)

Sollte eine Filterung für manche Dateitypen oder für manche Accounts nicht möglich sein, dann sollten zumindest potentiell gefährliche Anhänge prominent als "Gefahr" markiert werden.

Des weiteren kann auch bereits die Annahme von Spams am Mail-Server reduziert werden:

- Implementierung von SPF (Sender-Policy-Framework) auf dem SMTP-Server helfen, bereits die Annahme von nicht legitimen E-Mails zu reduzieren. Hierbei ist jedoch zu prüfen, ob signifikante Seiteneffekte auftreten, die eigentlich gewünschte E-Mail-Kommunikation unterbinden.
- Greylisting verhindert effektiv die Zustellung von E-Mails von den meisten Spam-Bots.
- Auch sollte der eigene E-Mail Server die Annahme von E-Mails mit internem Absender (SMTP-Envelope und From-Header) von Extern ablehnen (Anti-Spoofing)

4.1.5 Netzwerklaufwerke

Nutzer sollten wichtige Daten immer auf Netzlaufwerken ablegen, die in eine zentrale Datensicherung eingebunden sind. Wichtige Dokumente sollten nie nur lokal abgelegt werden.

Netzlaufwerke bieten als Vorteil, dass Zugriffsrechte auf Need-to-know Basis vergeben werden können. Auch ist es möglich, diese nachträglich zu verändern. So können zum Beispiel den Nutzern die Schreibrechte auf archivierte alte Projektdaten entzogen werden. Dadurch bleiben die Daten noch im Zugriff, eine Verschlüsselung durch einen Ransomware-Trojaner wäre aber nicht mehr möglich.

4.1.6 Netzwerke segmentieren

Eine Netzsegmentierung hilft Schäden zu begrenzen, da eine Ransomware nur die Dateien verschlüsseln kann, auf die das ausführende Nutzerkonto, Lese- und Schreibrechte hat. Hierbei ist insbesondere auch die sichere Verwendung von Administrator Accounts (s.o.) notwendig , weil ansonsten das Konzept fällt.

4.1.7 Remotezugänge sichern

Wie bereits bei den Angriffsvektoren beschrieben, versucht eine Angreifergruppe Ransomware über kompromittierte Remote-Zugänge auf Systemen zu installieren. Daher sollten auch der Zugriff von Außen abgesichert werden. In der Regel sollten diese immer über VPNs, zusammen mit einer Zwei-Faktor-Authentisierung geschützt werden. Zusätzlich können auch Quell-IP-Filter und ein Monitoring die Absicherung unterstützen.

Bei der Absicherung von Außen helfen auch Penetrationstests, die von außen erreichbare Systeme finden und auf ihre Sicherheit prüfen können.

4.1.8 Sicherer Umgang mit Administrator Accounts

Grundsätzlich sollten mit privilegierten Accounts nur Administratorentätigkeiten durchgeführt werden. Es sollten mit diesen Accounts keine E-Mails gelesen und nicht im Internet gesurft werden. Dafür benötigen Admins normale Userkonten. Dies sollte über Gruppenrichtlinien durchgesetzt werden.

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

Ein privilegiertes Konto sollte immer über eine Zwei-Faktor-Authentisierung geschützt werden.

4.1.9 Virenschutz

Neue Versionen von Schadsoftware werden nur selten sofort über normale AV-Signaturen erkannt. Daher sollten bei professioneller Antivirensoftware konsequent alle verfügbaren Module genutzt werden. Die meisten Infektionen mit neuen Varianten von Ransomware werden durch die Intrusion Prevention (IPS)-Module und Cloud-Dienste der AV-Software verhindert. Dies ist auch der Grund, warum die Erkennung infizierter Dateien an Gateways sehr viel schlechter ist, als bei den Viren-Schutzprogrammen für Endgeräte. An Gateways sollten zusätzlich Black- / Whitelisting-Dienste genutzt werden, die Verbindungen zu bösartigen URLs unterbinden.

Häufig kann über Module zur Anwendungskontrolle die Ausführung oder Verbreitung der Malware verhindert werden, indem diese verdächtiges und typisches Verhalten von Malware unterbindet. Wenn Malware eines bestimmten Typs z. B. immer die gleichen Verzeichnisse benutzt, um ihre Dateien zu speichern, kann die Ausführung von Dateien in diesen Verzeichnissen blockiert werden. Wer einen entsprechenden Supportvertrag abgeschlossen hat, sollte in jedem Fall bei seinem AV-Hersteller aktiv nach zusätzlichen Schutzmöglichkeiten und Konfigurationshinweisen nachfragen.

Da diese zusätzlichen Maßnahmen möglicherweise auch legitime Applikationen blockieren, empfiehlt es sich, neue bzw. verschärfte Regeln zuerst im „Log-only-Modus“ zu betreiben und nach einer ausreichenden Testphase die Protokolldaten der AV-Software zu prüfen. Wenn legitime Applikationen von einer Regel berührt werden, können diese Anwendungen über ein Whitelisting von der Regel ausgenommen werden.

Da nicht nur Windows-Systeme erfolgreich angegriffen werden, sollten unabhängig vom Betriebssystem (sofern verfügbar) professionelle Viren-Schutzprogramme für den Enterprise-Bereich in Unternehmen und Institutionen eingesetzt werden. Nur Enterprise-Produkte bieten ausreichende

Konfigurationsmöglichkeiten und die Möglichkeit zur zentralen Administration. Unabhängig von Signaturupdates sollte immer die neueste Programmversion eingesetzt werden, da neue und verbesserte Erkennungsverfahren häufig nur in die aktuelle Version integriert werden.

4.2 Backups / Datensicherungskonzept

Ein Backup ist die wichtigste Schutzmaßnahme, mit der im Falle eines Ransomware-Vorfalls die Verfügbarkeit der Daten gewährleistet ist. Jede Institution sollte über ein Datensicherungskonzept (IT Grundschutz: B 1.4 Datensicherungskonzept) verfügen und dieses auch umsetzen.

Insbesondere müssen die Daten in einem Offline-Backup gesichert werden, da viele Ransomware-Varianten auch Online-Backups, wie Daten auf NAS-Systemen oder Schattenkopien, verschlüsseln.

Zu einem Backup gehört auch immer die Planung und Vorbereitung des Wiederanlaufs und der Rücksicherung der Daten.

4.3 Awareness / Schulungen / Mitarbeitersensibilisierung

In Awareness-Kampagnen und in der Schulung von Mitarbeitern wird immer auf zwei ganz wesentliche Infektionswege für Schadprogramme hingewiesen:

- Einschleusen durch unbedarftes Öffnen von Anhängen in E-Mails
- Besuch kompromittierter Web-Seiten im Internet (Drive-By-Exploits)

Bei Ransomware, die in E-Mail-Anhängen verbreitet wird, werden infizierte Anhänge geöffnet wird, die Schadsoftware auf dem Rechner installiert. Einige der derzeit bekannten Varianten von Ransomware versenden nach der Installation E-Mails an alle Adressaten im Adressbuch. Dies ist ein sehr perfider Angriff, weil die Empfänger der schadhaften E-Mail die Absender kennen und somit vorsätzlich das Vertrauen einer bekannten Person ausgenutzt wird. In der E-Mail-Kommunikation ist dauerhaft besondere Vorsicht geboten, weil E-Mails mit schadhafter Software nicht ausschließlich von unbekannten Absendern kommen. Daher sollen E-Mails immer vor dem Öffnen eines Anhangs gelesen und auf Echtheit überprüft werden. Es sollten auf keinen Fall Anhänge von E-Mails unbekannter Absender geöffnet werden.

Oft enthalten E-Mails keine Anhänge, sondern im Text werden „Links“ zu weiterführenden Informationen im Internet angeführt. Durch einen Klick auf den Link öffnet der Browser die entsprechende Seite im Internet. Ransomware kann auch bereits über den einfachen Besuch einer kompromittierten Webseite auf den Rechner gelangen. In diesen Fällen wird die schädliche Software automatisch installiert, dies auch völlig unmerklich für den Nutzer. Diese Angriffe werden als „Drive-By-Exploits“ bezeichnet. Bleiben Sie vorsichtig, bei zweifelhaften Kommunikationspartnern und insbesondere bei Links in E-Mails, halten Sie Ihre Neugierde im Griff, und folgen nur bei absoluter Sicherheit dem Link.

Ein gesundes Misstrauen zu allen Informationen im Internet und ein gesunder Menschenverstand bei allen Kontakten im Internet können Sie vor finanziellen und persönlichen Schäden bewahren, bleiben Sie kritisch. Die Technik ist nicht ohne Schwachstellen und Sicherheitslücken, dies ist jedoch nur ein Teil der Risiken bei Nutzung von PC, Smartphone und Internet. Dort, wo Angreifer aufgrund technischer Abwehr durch Firewalls und Virenscannern nicht erfolgreich sind, gehen sie andere Wege. Die Nutzer sind aufgrund einer Sorglosigkeit im Umgang mit der Informationstechnik gefährdet und daher oft auch leichte Beute.

Bekannt sind viele erfolgreiche Varianten des „Social Engineering“, in dem Angreifer eine persönliche Beziehung vortäuschen, Gewinne versprechen, mit günstigen Preisen locken und wohl wissend „Geiz frisst Hirn“ nicht selten das Interesse des Nutzer wecken und zu Fehlhandlungen verführen.

Vertrauen Sie nicht blind den Meldungen, den Nachrichten, klicken Sie nicht unbedarft auf noch so verlockende Angebote. Auch im Internet gibt es keine Ware kostenlos, Sie zahlen mit der Preisgabe persönlicher Daten, eine neue Währung im Internet. Sind der Absender, der Inhalt und Anhang einer E-Mail

plausibel? Ist das Format des Anhangs sicher oder doch eine getarnte ausführbare Datei? Sind Sie an einem Informationsangebot einer Internetseite sehr interessiert, haben jedoch Zweifel an der Integrität, dann kann das Impressum und ein Telefonkontakt mehr Sicherheit verschaffen. Bei merkwürdigen Nachrichten von Freunden empfiehlt sich ein Anruf. Bleiben Sie wachsam und vorsichtig.

4.4 Weitergehende Schutzmechanismen

Diese Schutzmechanismen bieten einen sehr hohen Schutz, erfordern aber in der Regel auch einen höheren Aufwand auf der Administrationsseite.

4.4.1 Maßnahmen zur Verhinderung der Ausführung unerwünschter Software

Ein Großteil aller 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%, wo Malware in der Regel beim herunterladen abgelegt wird, unterbunden.

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

- Ausführung von Skripten (z. B. *.bat, *.cmd, *.cs, *.reg, *.vbs, *.js) (temporär) verhindern.
- Grundsätzlich die Deaktivierung von Scriptinghost

4.4.2 EMET

Die Erfolgswahrscheinlichkeit von Angriffen kann durch Einsatz von EMET (Enhanced Mitigation Experience Toolkit) reduziert werden. EMET verhindert das Laden von bestimmten Modulen durch geschützte Applikationen. Konkret wird einem Prozess das Laden bestimmter DLLs untersagt. Zum Beispiel wird verhindert, dass Microsoft Word das Adobe Flash Plugin lädt. Mehr Informationen dazu finden sich in einer Veröffentlichung der Allianz für Cyber-Sicherheit: "Anwendungsschutz vor ungepatchten Schwachstellen mittels EMET".

4.4.3 Erkennung von Ransomwaredateien auf Fileservern

Mit dem Ressourcen-Manager für Datei-Server (File Server Ressource Manager) ist es möglich eine Dateigruppe mit der Endung *.* zu erstellen und eine Liste mit Ausnahmen zuzulassen (z. B. *.docx, *.xlsx, *.txt usw.). Damit wäre es, mit einer entsprechenden Dateiprüfungsregel möglich, das Erstellen von Dateien mit anderen Endungen als die in der Liste der Ausnahmen aufgezählten zu verhindern bzw. zu erkennen. Mit Hilfe der Möglichkeit zur Erzeugung von Ereignisprotokolleinträgen, könnte auch durch Verknüpfung solcher Ereigniseinträge mit entsprechenden Aufgaben ggfs. Maßnahmen - Skripte können aufgerufen werden - ergriffen werden.

Auf Linux Systemen ist eine ähnliche Alarmierung / Blockierung mit dem Paket Fail2Ban möglich. Dazu muss der Samba-Server so konfiguriert werden, dass alle Schreib- und Umbenenn-Aktionen protokolliert werden. Anschließend wird Fail2Ban so konfiguriert, dass wenn ein Nutzer zu viele Dateien auf einmal neu anlegt / umbenennt, ein Alarm ausgelöst wird. Gleichzeitig könnten diesem Nutzer auch die Schreibrechte

entzogen werden, wodurch eine weitere Verschlüsselung gestoppt würde. Eine Anleitung findet sich auf Heise[2].

4.4.4 Zentraler Logserver

Wenn es zu einem Vorfall kommt, kann die Auswertung von Logdaten dabei helfen, dessen Ausmaß festzustellen. Mit der Auswertung von zuvor erfassten Logdaten von Netzwerk-Kommunikation können Infektionen des Netzwerks festgestellt, infizierte Systeme entdeckt und idealerweise der initiale Infektionsweg identifiziert werden. Unternehmen sollten daher bereits im Vorfeld eine gut geplante Logging Policy etabliert haben und sicherstellen, dass die Logs auch regelmäßig erzeugt und mittels zentraler Logserver sicher gespeichert werden. Sollte keine Logging Policy im Unternehmen existieren, sollte dies umgehend nachgeholt werden.

4.4.5 Zugriffe auf Ransomware-C2 Server überwachen / blocken

In dem man Zugriffe aus dem eigenen Netz auf bekannte Ransomware Command & Control (C2) Server überwacht oder im besten Fall sogar blockiert, kann man sofort über kompromittierte Systeme alarmiert werden. Einige Ransomwarevarianten benötigen darüber hinaus eine Verbindung zu C2 Servern, bevor die Daten verschlüsselt werden können. In diesen Fällen wird sogar die Verschlüsselung der Daten unterbunden.

Das Ransomware-Tracker Projekt von Abuse.Ch bietet Echtzeit-Informationen zu aktiven Ransomware C2-Servern, sowie auch zu kompromittierten Seiten, die Nutzer mit Ransomware infizieren.

4.4.6 Schwachstellenscan und Penetrationstest

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 Schwachstellen-Scans soll insbesondere darauf geprüft werden, ob Aktualisierungen für Betriebssysteme, Browser und andere Anwendungen laufend eingespielt werden.

Eine entsprechende Überprüfung kann auch durch ein externes Beratungsunternehmen durchgeführt werden. 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.

4.4.7 Übungen

Übungen sind ein vielfältig einsetzbares Mittel. Schon einfache Übungen können sensibilisieren oder dazu beitragen, am grünen Tisch zu überprüfen, wie eine Institution mit einem Vorfall umgehen 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 auf einen Ransomware-Befall kann die Musterübung "Betroffen" (ACS interner Bereich) mit geeigneten Anpassungen verwendet werden. Dies ist eine Planbesprechung, bei der Institutionen die eigenen Prozesse im Falle einer Ransomware-Infektion beüben können.

2 https://www.heise.de/security/artikel/Erpressungs-Trojaner-wie-Locky-aussperren-3120956.html

5 Reaktionsmaßnahmen

Wenn es trotz der oben beschrieben Präventionsmaßnahmen zu einem Sicherheitsvorfall mit Ransomware kommt, gilt es ruhig zu bleiben und bedacht zu handeln. Im folgenden sind einige Maßnahmen aufgezählt, die im besonderen bei einem Ransomware-Vorfall zu beachten sind.

Grundsätzlich hilft für die Vorbereitung für einen Sicherheitsvorfall auch die Umsetzung des BSI Standard 100-4 "Notfallmanagement".

5.1 Lösegeldforderung

Bei Ransomware handelt es sich wie der Name es beschreibt um Lösegelderpressung durch die Organisierte Kriminalität. Das BSI kann nur nachdrücklich raten:

angemessen vorsorgen, im Schadensfall auf die Vorbereitungen zurückgreifen und NICHT zahlen.

Jede erfolgreiche Erpressung zeigt den Erfolg des Angriffs und motiviert den Angreifer weiter zu machen. Sie finanziert die Weiterentwicklung der Schadsoftware und fördert deren größeren Verbreitung. Mit jeder bezahlten Infektion steigt damit die Wahrscheinlichkeit für den Betroffenen noch einmal, vielleicht sogar über raffiniertere Verfahren, infiziert zu werden. Es gibt keine Garantie, dass die Verbrecher auch ihr "Wort halten" und die Entschlüsselung ermöglichen. Auch solche Fälle sind bekannt.

5.2 Anzeige erstatten

Ein wichtiger Punkt ist es, polizeilich Strafanzeige zu erstatten.

Polizeiliche Ermittlungen ermöglichen weitergehende Untersuchungen, die Unternehmen und CERTs nicht durchführen können: z. B. dem Fluss der gezahlten Lösegelder zu folgen, durch Überwachungen von C&C-Servern Informationen zu gewinnen, aus dem Ausland agierende Täter zu verfolgen oder Systeme vom Netz zur Auswertung zu beschlagnahmen oder zu "sinkholen".

Letztlich kann das Geschäftsmodell Ransomware nur durch Fahndungsdruck zerstört werden und die Täter auf diesem Weg identifiziert und "von der Straße geholt werden", damit keine weiteren Straftaten begangen werden können.

Die Bundesländer bzw. die zuständigen Landeskriminalämter haben Anlaufstellen eingerichtet, die Unternehmen, welche Opfern von Cyber-Straftaten geworden sind, beratend zur Seite stehen und bei einer Anzeige unterstützen. Eine Liste der Anlaufstellen, sowie eine Broschüre[3] zum Thema finden Sie auf den Webseiten der Allianz für Cybersicherheit.

Privatpersonen können bei der nächsten lokalen Polizeidienststelle Anzeige erstatten.

5.3 Incident Response

Zur Begrenzung des möglichen Schadens sollten infizierte Systeme zunächst umgehend vom Netz getrennt werden. Am schnellsten geht dies durch die Trennung des Netzwerkkabel vom Computer und die Abschaltung etwaiger WLAN-Adapter.

Bei der Identifikation der betroffenen Systeme helfen Logdaten, anhand derer bspw. Zugriffe auf Netzwerklaufwerke erkannt werden können. Auch die Metadaten der verschlüsselten Dateien, z.B. welche Nutzeraccounts die Dateien erzeugt haben, können Hinweise auf infizierte Systeme liefern.

3 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/ZAC/polizeikontakt.html

Es muss sehr früh entschieden werden, ob eine forensische Untersuchung durchgeführt wird. 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. Sollten keine Erfahrungen mit der forensischen Sicherung des Arbeitsspeichers bzw. der Festplatte im Unternehmen existieren, sollte ein Experte hinzugezogen werden.

Bevor mit der Datenwiederherstellung begonnen wird, ist eine Neuinstallation des infizierten Systems erforderlich. Das verwendete Betriebssystem sollte von einem vertrauenswürdigen Datenträger stammen.

Unter bestimmten Voraussetzungen ist auch ohne Datensicherung via Backup eine teilweise oder komplette Wiederherstellung der Daten möglich. Eine Entschlüsselung kann u. U. funktionieren, wenn

- die Ransomware Schattenkopien in Windows nicht verschlüsselt oder gelöscht hat,
- Snapshots von virtuellen Maschinen oder
- bei Clouddiensten frühere Dateiversionen existieren,
- die forensische Wiederherstellung gelöschter Dateien möglich ist bzw.
- die Ransomware in ihrer Verschlüsselungsfunktion Fehler aufweist.

In der Regel sollte man sich aber nicht auf das Funktionieren dieser Möglichkeiten verlassen.

Zusammengefasst sollte das Incident Response die folgenden Ziele verfolgen:

- Schäden begrenzen
- Infektionsvektor finden und schließen um eine erneute Infektion zu verhindern
- Systeme neu aufsetzen und Daten wiederherstellen

Externe Expertise

Falls betroffene Unternehmen kein eigenes IT-Security Team / Computer Emergency Response Team (CERT) haben, welches den Vorfall bewältigen kann, wird empfohlen, sich externe Unterstützung durch eine Fachfirma einzukaufen.

Auf den Webseiten der ACS finden Sie eine Übersicht über durch das BSI zertifizierte IT-Sicherheitsdienstleister[4] für IS-Revision und IS-Beratung sowie Penetrationstests.

Opfer von Ransomware können auch im Forum der Botfrei Initiative Unterstützung erhalten. Dort beantworten Experten des Anti-Botnetz Beratungszentrums[5] Fragen von Betroffenen.

4 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/zert_dienstleister/zertdienstleister.html

5 https://blog.botfrei.de/forums/

6 Weitere Informationen

Hier finden Sie eine lose, nicht abschließende Auflistung von Informationen zum Themenkomplex Ransomware.

6.1 Produkte des BSI

6.1.1 Öffentlich

Pressemitteilungen:

- IT-Sicherheitsvorfälle beeinträchtigen Funktionsfähigkeit Kritischer Infrastrukturen: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/Funktionsfaehigkeit_Kritischer_Infrastrukturen_08032016.html
- Krypto-Trojaner: Backups schützen gegen Datenverlust: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/Krypto-Trojaner_22022016.html
- Safer Internet Day: BSI informiert über Risiken durch Ransomware: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/SaferInternetDay_Ransomware_05202016.htm

Mediathek:

n-tv Interview mit dem BSI Präsidenten zum Thema "Locky" - https://www.bsi.bund.de/DE/Presse/Mediathek/mediathek_node.html

6.1.2 Bundesverwaltung, Verwaltungs-CERTs, Teilnehmer des UP KRITIS / der Allianz für Cyber-Sicherheit

Den oben genannten Gruppen stehen darüber hinaus eine Reihe von Informationen zur Verfügung, die über die üblichen Verteilwege bereits verteilt oder nachrecherchierbar sind. Dazu gehören unter anderem:

- BSI Cyber-Sicherheits Warnmeldungen (TLP Green)
- BSI Cyber-Sicherheits Vorfallsinformation (TLP Green)
- BSI Themenlagebilder (TLP Green)
- BSI Musterübungen (TLP Green)

Hinweis: Jedes Unternehmen bzw. jede Institution in Deutschland kann über eine kostenlose Mitgliedschaft in der Allianz für Cyber-Sicherheit[6] Zugriff auf die genannten Dokumente erhalten.

6.2 Externe Informationen

6.2.1 Anti Botnetz Beratungszentrum

Das Anti Botnetz Beratungszentum stellt diverse Hilfen für Betroffene bereit:

https://www.botfrei.de/

6 https://www.allianz-fuer-cybersicherheit.de

Hilfe bei Ransomware

- https://blog.botfrei.de/2016/01/ransomware-was-nun/
- https://blog.botfrei.de/2016/02/massnahmen-gegen-die-ransomware-locky/
- https://blog.botfrei.de/?s=ransomware
- http://bka-trojaner.de/

Expertenberatung im Forum

- https://blog.botfrei.de/forums/

Zuordnung Dateiendung zur Ransomware

- https://blog.botfrei.de/forums/topic/ransomware-verschluesselt-dateien-und-fordert-zur-zahlung-von-50e-auf/#post-68168

Abuse.ch Ransomware Tracker

Der Betreiber der Webseite Abuse.ch hat am Anfang März 2016 den Ransomware Tracker gestartet. Über Blocklisten und einen RSS-Feed werden bekannte Command & Control Server der Ransomware Familien CryptoWall, TeslaCrypt, TorrentLocker, PadCrypt, Locky, CTB-Locker, FAKBEN verteilt.

- https://www.abuse.ch/?p=9144
- https://ransomwaretracker.abuse.ch/

CERTs, Security Dienstleister und Presse (Beispielhaft)

CIRCL.LU: TR-41 - Crypto Ransomware – Vorsichtsmaßnahmen und Verhalten im Infektionsfall
http://circl.lu/pub/tr-41/de/

US-CERT: Alert (TA14-295A) Crypto Ransomware
https://www.us-cert.gov/ncas/alerts/TA14-295A

Sophos: Sofortmaßnahmen gegen Krypto-Trojaner - https://www.sophos.com/de-de/medialibrary/Gated%20Assets/white%20papers/Sophos-emergency-measures-against-crypto-Trojan-wp.pdf?la=de-DE

GData: Verschlüsselungs-Trojaner Locky: Das sollten Sie jetzt wissen -
https://blog.gdata.de/2016/02/25206-verschlusselungs-trojaner-locky-das-sollten-sie-jetzt-wissen

Heise: Erpressungs-Trojaner wie Locky aussperren - Samba-Server mit fail2ban zusätzlich sichern -
http://heise.de/-3120956

Stop panicking about the Locky ransomware
http://robert.penz.name/1252/stop-panicking-about-the-locky-ransomware/