Bundesamt
für Sicherheit in der
Informationstechnik

Ransomware

Bedrohungslage, Prävention & Reaktion 2021

CERT-Bund
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 (v.a. durch Verschlüsselung) 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.

In den letzten Jahren 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 einer „Strafzahlung“ wieder freigegeben wird.

Im Laufe der Zeit wurden 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 in der Regel 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 und Monero oder anonymen Guthaben- und Bezahlkarten kommt. Im Vergleich zu Cyber-Angriffen über Banking-Trojaner sind weder Mittelsmänner für Überweisungen noch Warenagenten notwendig, um einen erfolgreichen Angriff zu monetarisieren.

Für das Opfer ist der wesentliche Unterschied gegenüber einer Betroffenheit mit klassischer 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 nicht nur "etwas langsamer" weil im Hintergrund Dritte angegriffen werden.

Stattdessen sind zum Beispiel die Kinderbilder, Familienfotos und alle Kontakte verloren oder die Unternehmensdaten nicht mehr zugreifbar oder kritische Dienstleistungen nicht mehr verfügbar. Es helfen meist nur präventive Maßnahmen und insbesondere Offline-Backups.

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

Über die bisherige Entwicklung von Ransomware wird im Anhang 8.1 berichtet. Eine mögliche zukünftige Entwicklung der Ransomware wird im Anhang 8.2 behandelt.

2 Bedrohungslage

Ransomware ist ein für Cyber-Kriminelle ein seit Jahren etabliertes Geschäftsmodell und betrifft Desktop-Betriebssysteme wie Microsoft Windows und Apple Mac OS, sowie Server-Systeme unter Windows und Linux. Seit 2016 hat sich die Bedrohung verschärft.
Infektionsvektoren von Ransomware sind aktuell E-Mail-Anhänge oder Spam-Mails mit verlinkter Schadsoftware, sowie Schwachstellen in aus dem Internet erreichbaren Server-Systemen.

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

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

2.1 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 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. Teilweise wurden die Dateien in einem Archiv (meist ZIP) ausgeliefert, welches mit einem in der Spam-Mail stehenden Passwort verschlüsselt war.

Unter anderem war seit September 2019 bis zum Takedown durch Strafverfolgungsbehörden das Netzwerk um den Trojaner Emotet aktiv. Dieser spähte z.B. Outlook Kontakte und E-Mails aus und verteilte Schadprogramme, indem die Spam-Mails als vermeintliche Antworten auf zuvor ausgespähte tatsächliche E-Mails versendeten. Die bekannten Betreffzeilen und Zitate einer vorhergehenden Kommunikation ließen die gefälschten E-Mails für die Empfänger noch authentischer erscheinen. Entsprechende Verteilung mit echtem Text in der E-Mail wird aber auch von anderer Schadsoftware genutzt. Emotet lud im Auftrag anderer Tätergruppen andere Schadprogramme wie z.B. Trickbot nach, welches wiederum die Ransomware Ryuk verteilen kann.

Mittlerweile wird die Methode des Social Engineerings mittels gestohlen E-Mails durch andere Tätergruppen aufgegriffen. Die Bedrohung bleibt daher bestehen.

2.1.2 Drive-By Infektionen mittels Exploit-Kits

Exploit-Kits gehören seit mehreren Jahren ebenfalls zu den Infektionsvektoren für Schadsoftware. Neue Exploits für Schwachstellen in weit verbreiteten Programmen werden binnen kürzester Zeit in Exploit-Kits integriert und auch zur Verteilung von Ransomware oder anderen Schadprogramm-Typen verwendet. Aber auch andere Schwachstellen in nicht aktueller Software wie dem Browser oder dem Flash Player werden hierfür ausgenutzt.

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.

Durch ein gutes Patchmanagement lassen sich Drive-By Infektionen relativ einfach verhindern.

2.1.3 Schwachstellen in Servern

Stellt das Opfer selbst einen Server bereit, der aus dem Internet zu erreichen ist, so können Täter durch Ausnutzung von Schwachstellen oder Erraten von schwachen Passwörtern in diesen eindringen. Die große Zahl an in den vergangenen Jahren veröffentlichten Zugangsdaten erhöht die Wahrscheinlichkeit, dass Täter im Besitz noch anwendbarer Zugangsdaten sind. Diese können Täter für zum Beispiel Credential Stuffing oder Brute-Force Angriffe missbrauchen.

Als Schutz vor entsprechenden Angriffen hilft beispielsweise die konsequente Verwendung von zweiten Faktoren.

Nicht schnell genug geschlossene Schwachstellen in Server-Programmen wie etwa VPN-Software oder Microsoft Exchange werden immer wieder von Angreifern ausgenutzt. Teilweise wird sich auch kurzfristig ein Zugang verschafft und Monate später für weitere Aktionen ausgenutzt.

2.1.4 Ungeschützte Fernzugänge

Bei Vorfällen mit Infektionen wurde in einigen Fällen ein zusätzlicher Modus Operandi der Täter festgestellt. Diese scannen das Internet aktiv nach Systemen, welche Fernzugänge ins Internet anbieten, wie zum Beispiel Microsoft Remote-Desktop (RDP). Dort führen sie Brute-Force Angriffe auf das Passwort durch. Bei einem erfolgreichen Login installieren sie z.B. die Malware Trickbot und Ransomware Ryuk.

Die unter dem Namen „Shitrix“ bekannt gewordene Citirx-Schwachstelle wurde etwa ausgenutzt um verschiedene Institutionen anzugreifen.

2.2 Ransomware Varianten

Für Institutionen sind derzeit insbesondere die folgenden Ransomware-Varianten relevant:

- Ryuk
- REvil / Sodinokibi
- DoppelPaymer
- Egregor (Seite 14)
- Clop
- Conti
- Darkside
- Defray777

- IEncrypt / BitPaymer

Hier erfolgt üblicherweise die Erstinfektion über eine andere Schadsoftware, wie z.B. Emotet. Wie oben dargestellt sind aber auch Infektionen über schlecht geschützte RDP-Dienste bekannt. Der Erstzugang zu einem System kann anschließend an andere Gruppen weiterverkauft werden, die dann versuchen mittels Ransomware Gewinn zu erzielen. Es erfolgt hier teilweise eine „Arbeitsteilung“ im kriminellen Bereich, welches als Cybercrime-as-a-Service bekannt ist.

2.3 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 einem 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. Wenn im Rahmen von Datenveröffentlichungen Rechnungen veröffentlicht werden, kann dies etwa Einblick in die Vertragsgestaltung aller Beteiligten geben (siehe auch Kapitel 2.4).

Das Schadensausmaß ist erheblich davon abhängig, wie die betroffene Organisation technisch und organisatorisch vorbereitet ist: Selbst wenn Präventivmaßnahmen nicht gegriffen haben und die Störung nicht abgewendt werden konnte, kann eine gute Bewältigungsstrategie den Schaden erheblich begrenzen. Eine 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 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, weil ihre lokalen Datenbasis beschädigt wurde. 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 à jour zu bekommen. Im schlimmsten Fall muss nach einer Infektion mit Zugriff auf das Active Directory die komplette Domäne neu aufgebaut werden, was abhängig von der Komplexität einen enormen Aufwand bedeuten kann.

2.4 Veröffentlichung von Daten

Verschiedene Cybercrime-Gruppierungen leiten vor der Verschlüsselung häufig auch noch Daten aus. Diese werden dann teilweise veröffentlicht, um den Druck auf das Opfer zu erhöhen. Üblicherweise erfolgt eine Bekanntgabe des Opfers auf der jeweiligen Webseite der Täter mit dem Hinweis, wie viele und welche Daten abgeflossen sind.

Aber auch direktere Drohungen sind bekannt: So wurden beispielsweise bei einem Angriff auf eine Psychotherapie-Klinik in Finnland den Patienten gedroht, dass Daten zu ihnen veröffentlicht werden, sollte die Klinik nicht bezahlen.[1]

Ein entsprechendes Bedrohungsszenario ist auch mit Geschäftsgeheimnissen denkbar, bei denen Konkurrenten entsprechende Informationen auf keinen Fall erhalten dürfen, etwa Vertragskonditionen.

1 https://www.golem.de/news/finnland-datenleck-von-psychotherapie-klinik-fuer-erpressung-genutzt-2010-151742.html

2.5 Motivation des Angreifers

Die erste und wichtigste Motivation für die Verbreitung von Ransomware ist der *finanzielle Gewinn*. Forderungen die erfüllt werden, ermuntern einen Täter bei ähnlich gelagerten folgenden Fällen eine höhere Forderung zu stellen. Nicht unwesentlich tragen auch Versicherungen zur Erhöhung der Lösegeldzahlungen bei. Einige Institutionen besitzen eine entsprechende Cyber-Versicherung, haben aber lückenhafte Sicherungssystem. Diese können also nicht davon ausgehen, ihr System aus eigener Kraft wieder voll funktionsfähig aufzusetzen, da Backups ganz fehlen, lückenhaft sind oder die Einspielung fehlschlägt. Hierbei ist zu beachten, dass Cyber-Versicherungen häufig Haftungsausschlüsse haben, wenn die Absicherung nicht dem Stand der Technik entspricht. Solche Institutionen zahlen aufgrund einer bestehenden Versicherung auch hohe geforderte Summen, weil die Hoffnung auf eine schnelle Lösung die negativen Aspekte übersteigt. Zu diesen negativen Aspekten zählt beispielsweise eine Verteuerung bzw. Ablehnung der weiteren Versicherung, ein Reputationsverlust oder die Finanzierung der Ransomware-Szene und damit künftiger Angriffe.

Das Opfer befindet sich in einem klassischen aus der Spieltheorie bekannten "Gefangenen-Dilemma": Kooperation (und damit nicht zahlen) würde allen helfen, aber man erwartet aus der Ablehnung der Kooperation, Verrat, Vorteile für sich.

Die Kooperation eines Opfers mit allen anderen Opfern würde eine konsequente Zahlungsverweigerung bedeuten. In diesem Fall würde kein Täter jemals Gewinne aus der Erpressung erhalten. Dem Opfer entstehen hiervon unberührt zunächst dennoch Schäden durch den Ausfall und die Erneuerung seiner Systeme. Langfristig würde eine konsequente Zahlungsverweigerung jedoch die Motivation, weitere Ransomware in Umlauf zu bringen, senken. In jedem Fall würde ein geschlossenes Vorgehen für Angreifer einen viel geringeren Aufwand für Aktionen rechtfertigen, bei denen es primär um finanziellen Gewinn geht. Die oben geschilderte Reaktion eines Opfers, nämlich Lösegeld zu zahlen, entspricht dabei dem Verrat gegenüber anderen Opfern. Diese werden durch die erhöhte Motivation der Täter wahrscheinlicher einem neuen Ransomware-Angriff ausgesetzt sein.

Das BSI beobachtet bei Ransomware-Vorfällen eine zunehmende Fokussierung auf Unternehmen. Diese Entwicklung ist ebenfalls von der Erwartung erhöhter Lösegelder getrieben, da man eine Abhängigkeit von verschiedenen Parametern annehmen kann:

- Die *Anzahl der in einem Netz erreichbaren Rechner*, die einer IT-Administration unterliegen, ist proportional zu dem Aufwand, der nach einem Angriff getrieben werden muss, um den Schaden wieder zu beheben.
- Das innerhalb eines Netzes verfügbare Personal *für die IT-Administration und IT-Sicherheit ist oft klein*. Sie möchte daher möglichst *homogene Strukturen*, um eine einfache Verwaltung zu ermöglichen. Die Angreifer können damit teilweise viele Systeme auf einmal lahmlegen.
- Der *Wert der Daten*, die in einem Firmennetz oder einem Netz der öffentlichen Verwaltung gespeichert sind, kann mit der Anzahl der Mitarbeiter, dem zu erwartenden Gewinn, oder Aufwand skalieren, den es bedeuten würde, die Daten wiederherzustellen. Während Firmen beim Verlust der Daten Gefahr laufen insolvent zu werden, sind öffentliche Stellen oft gezwungen alle Mittel aufzuwenden, die Daten wiederherzustellen.

Täter sind also motiviert Institutionen anzugreifen, die Netze mit vielen Rechnern besitzen, wenig oder mangelhaft ausgebildetes IT-Personal haben, homogene Strukturen verwenden, wertvolle Daten verwalten und möglichst noch versichert sind, um hohe Lösegelder fordern zu können.

Eine weitere Motivation zur Verbreitung von Ransomware ist die *Sabotage*. Diese kann *politisch* oder *wirtschaftlich* getrieben sein, was maßgeblichen Einfluss auf die Opferwahl und das Vorgehen im Einzelfall hat. In jedem Fall steht allerdings die Schädigung des Opfers im Vordergrund. Im Beispiel NotPetya, eine Ransomware die 2017 in der Ukraine und international großen Schaden anrichtete, ging bei den Betroffenen keine Erpressungsmeldung ein und den Nutzern wurde keine Möglichkeit gegeben, die verschlüsselten Dateien zu entschlüsseln. Allerdings gibt es auch aktuelle Fälle wie bei der Ransomware Ordinypt und GermanWiper, bei denen Lösegeldforderungen gestellt wurden, obwohl die Schadsoftware

Nutzerdaten lediglich mit Nullen überschrieb, so dass eine Entschlüsselung technisch gar nicht möglich war. Dies legt nahe, dass die Opfer dazu verleitet werden sollten, ohne Kenntnis über die Sachlage Lösegeld zu zahlen, obwohl ihre Daten unwiderruflich zerstört wurden.

Es existieren Theorien, nach denen Staaten durch Lösegelderpressungen durch Ransomware Devisen einspielen wollen. Bei einem derartigen *politisch* motivierten Angriff ist es möglich, dass die Erpressung nicht die wesentliche Komponente ist. Wenn ein kombinierter Angriff wie der in Kapitel 8.1.4 geschilderten "Triple Threat Attack" verwendet wird, sind die Verbindungs- und Bankkontendaten wahrscheinlich wertvoller als das geforderte Lösegeld. In diesem Fall könnte die Erscheinung als Ransomware-Angriff als reine Tarnung bzw. Ablenkung dienen. Neben monetärer Gegenwerte sind hierzu auch andere für den Angreifer wertvolle Informationen zu zählen, deren Abfluss durch ein Ransomware-Angriff getarnt oder verschleiert werden soll. Die Erlangung derartiger Informationen kann auch wirtschaftlich motiviert sein.

Ein kleiner Teil der Ransomware-Angriffe ist anders motiviert. So wollen sich beispielsweise aufstrebende Hacker in der Szene bekannt machen oder einfach mit ihrem Können prahlen. Wenige Einsätze von Ransomware waren eher harmlos und schienen für Spiele werben zu wollen. Vereinzelt werden Ransomware-Angriffe auch von Hacktivisten eingesetzt, um einem für sie wichtigem Thema Nachdruck zu verleihen oder Geld für die weitere Operation ihrer Aktivitäten einzunehmen.

Zusammengefasst bestehen folgende Motivationen für die Verbreitung von Ransomware:

- Finanzielle Gewinne
- Sabotage (politisch, wirtschaftlich)
- Ablenkung
- Aufmerksamkeit/"Werbung" für Spielebereich
- Erreichung von Zielen von Hacktivisten

3 Lage in den Unternehmen

Bei Ransomware-Vorfällen treten Versäumnisse bei der Prävention häufig deutlich zutage. Schlecht gepflegte Systeme, fehlende, veraltete oder nicht überprüfte Software-Backups, schwache Administrator-Passworte, fehlende Netzsegmentierung u.v.a.m. rächen sich bei Ransomware sofort durch die eingetretenen Schäden.

Auch das Verhalten der Mitarbeiter spielt eine zentrale Rolle. Einige Angriffe sind mittlerweile durch Nutzung legitimer Namen und Mails so gut, dass sie immer schwerer zu erkennen sind. Andere der beobachteten Ransomware-Spamwellen sind hingegen nicht mit großem Aufwand gestaltet. Hier würde eine Sensibilisierung der Mitarbeiter helfen.

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 normale Schutzmaßnahmen vereitelt werden.

Die Zahl der Angriffe haben in 2020 im Vergleich zum Vorjahr nicht noch weiter zugenommen, haben aber mit der verstärkten Androhung von Veröffentlichung der Daten ein neues Gefahrenpotential für die Betroffenen.

Weitere Fälle sind im Anhang 8.3 dargestellt. **Für diese Fallsammlung wurden ausschließlich Informationen öffentlicher Quellen genutzt!**

3.1 Große Unternehmen

In diesem Kapitel wird über einige wenige herausgehobene Vorfälle berichtet.

In Deutschland fehlen bisher zum Glück noch große Ransomware-Infektionen. International hat es allerdings schon größere Unternehmen getroffen.

Norsk Hydro

Der norwegische Aluminiumkonzern Norsk Hydro ist in der Nacht zum 19. März 2019 Opfer eines Ransomware-Angriffs geworden. Norsk Hydro hat weltweit nach eigenen Angaben 35.000 Mitarbeiter in 40 Ländern und erwirtschaftete 2017 einen Umsatz von ca. 11 Mrd. Euro. Das Kerngeschäft von Norsk Hydro ist die Aluminiumproduktion, daneben gehört das Unternehmen zu den drei größten Stromerzeugern Norwegens.

Es wurde festgestellt, dass die IT-Systeme in den meisten Geschäftsfeldern von Norsk Hydro betroffen sind. Die Anlagen wurden zunächst als erste Reaktion vom Netz genommen und die Produktion wurde weitestgehend auf manuellen Betrieb umgestellt. Es wurde Lösegeld in unbekannter Höhe gefordert, aber von Norsk Hydro nicht gezahlt. Das Unternehmen nutzte stattdessen die vorhandenen Backups, um den Betrieb wiederherzustellen. Die Webseite war als Folge der Angriffe zeitweise nicht mehr erreichbar. Noch vier Wochen nach dem Vorfall wurden viele Bereiche manuell betrieben.

Beim Angriff kam die Ransomware "LockerGoga" zum Einsatz. Pressemitteilungen zufolge gab es im Vorfeld Manipulationen des Active Directory und den Austausch von Admin-Passwörtern, Abmeldungen eingeloggter Nutzer und die Deaktivierung von Netzwerkgeräten. Damit kann von einem gezielten Angriff mit individueller Vorbereitung auf das konkrete Opfer ausgegangen werden. LockerGoga war erstmals

Anfang des Jahres bei einem französischen Unternehmen eingesetzt worden und kurz nach der Attacke auf Norsk Hydro noch bei zwei US-Unternehmen der chemischen Industrie zum Einsatz gekommen.

Norsk Hydro ist nach eigenen Angaben alleine in der ersten Woche nach dem Cyberangriff ein wirtschaftlicher Schaden in Höhe von ca. 35 bis 43 Millionen US-Dollar entstanden. Während dieser Woche stand die Produktion in den am stärksten betroffenen Bereichen nahezu still.

Der Aluminiumpreis stieg in den ersten beiden Tagen nach dem Vorfall deutlich an. Der Kurs der Norsk Hydro Aktie selbst nahm keinen Schaden und stieg in der Folge sogar.

Norsk Hydro informierte die Öffentlichkeit und Börse umgehend (u. a. über Facebook) über den Cyberangriff. Am Tag nach der Attacke gab es eine Pressekonferenz und auch in den folgenden Wochen wurde die Öffentlichkeit über den Stand der Maßnahmen informiert. Das Unternehmen wurde für sein Vorgehen (keine Lösegeldzahlung, Backup-Nutzung, Informationspolitik) gelobt. Dieses Verhalten entspricht auch den Empfehlungen des BSI.

Quellen: [2],[3],[4],[5]

3.2 KMUs / Behörden

Universitätsklinikum Düsseldorf

In der Nacht vom 9. auf den 10. September 2020 kam es zu einem weitreichenden Ausfall der IT-Infrastruktur nach einem Ransomware-Angriff. Das UKD hat sich in der Folge von der Notfallversorgung abgemeldet und planbare sowie ambulante Operationen verschoben. Erst knapp zwei Wochen später, am 23. September. konnte das Klinikum wieder an der Notfallversorgung teilnehmen.

Einfallstor war hier eine Schwachstelle in einem VPN-Produkt. Ein Patch stand seit Januar 2020 bereit, eine eingebaute Hintertür der Angreifer ermöglichte einen Angriff aber noch nach mehreren Monaten.

Das BSI unterstützte mit einem mobilen Einsatzteam (MIRT) die Verantwortlichen des UKD auch vor Ort bei der Analyse und Bewältigung des Vorfalls

Obwohl das Klinikum offenbar nicht das eigentliche Ziel der Angreifer war und diese sogar den Schlüssel zur Entschlüsselung bereitgestellt haben, dauerte die „Aufräumaktion“ mehrere Wochen.

Quellen: [6],[7],[8],[9]

Funke Mediengruppe

Am 22. Dezember 2020 wurde bekannt, dass die Funke Mediengruppe von der Ransomware DoppelPaymer angegriffen worden war. Betroffen waren potentiell über 6.000 infizierte Systeme an bundesweit zahlreichen Standorten.

2 https://www.spiegel.de/netzwelt/netzpolitik/norsk-hydro-hackerangriff-war-eine-lockergoga-ransomware-attacke-a-1258627.html
3 https://www.kaspersky.de/blog/hydro-attacked-by-ransomware/18804/
4 https://www.hydro.com/nl-nl/media/news/2019/update-on-cyber-attack-march-26/
5 https://www.inside-it.ch/articles/53971
6 https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/krankenhaus-derzeit-nur-sehr-eingeschraenkt-erreichbar-patientenversorgung-eingeschraenkt
7 https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/uniklinik-duesseldorf-wieder-bereit-fuer-notfaelle
8 https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/UKDuesseldorf_170920.html
9 https://www1.wdr.de/nachrichten/rheinland/uniklinik-duesseldorf-erpressung-hacker-100.html

Kurzfristig konnten nur Notausgaben erstellt werden, kostenpflichtige Inhalte wurde frei erreichbar geschaltet. Bei diversen Magazinen und Zeitungen im deutschsprachigen Raum kam es in der Folge zu Lieferschwierigkeiten. Knapp eine Woche nach Ausbruch der Ransomware konnten die Tageszeitungen wieder in größeren Auflagen erscheinen.

Die zuständige Polizei Essen bildete eine Besondere Aufbauorganisation (BAO) und ermittelte mit dem LKA vor Ort.

Quellen: [10],[11],[12],[13],[14]

Egregor-Fallgruppe

Laut Digital Shadows soll es weltweit mindestens 71 Opfer der Ransomware Egregor geben. Auch in Deutschland gab es eine handvoll Betroffene. Unter den Betroffenen sollen auch Spieleentwickler und Publisher wie Crytek und Ubisoft sein.

Egregor droht, wie viele andere Ransomware-Gruppen auch, damit zuvor ausgeleitete Daten zu veröffentlichen. Nach eigenen Angaben werden Daten auch an Dritte „Kunden“ verkauft und nicht immer veröffentlicht.

Es wird vermutet, dass Egregor der Nachfolger der Ransomware Maze ist, deren „Betreiber“ angekündigt hatten den Betrieb einzustellen.

Quellen: [15],[16],[17]

10 https://www.heise.de/news/Trojaner-Angriff-Ransomware-legt-Funke-Mediengruppe-lahm-4998302.html
11 https://www.heise.de/news/Funke-Tageszeitungen-erscheinen-trotz-Hackerangriffs-wieder-in-groesseren-Umfaengen-5000289.html
12 https://www1.wdr.de/nachrichten/ruhrgebiet/hackerangriff-funke-mediengruppe-100.html
13 https://www.faz.net/aktuell/feuilleton/medien/cyberangriff-funke-mediengruppe-von-hackern-attackiert-17115147.html
14 https://hilfe.onleihe.de/pages/viewpage.action?pageId=16941113
15 https://www.digitalshadows.com/blog-and-research/egregor-the-new-ransomware-variant-to-watch/
16 https://unit42.paloaltonetworks.com/egregor-ransomware-courses-of-action/
17 https://www.bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/

4 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[18] für die Basis-Resilienz verwiesen.

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

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

5 Präventionsmaßnahmen

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

5.1 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.

5.1.1 Softwareupdates

Um generell vor Infektionen durch die Ausnutzung bereits behobener Sicherheitslücken geschützt zu sein, sollten Updates 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.

5.1.2 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. Nachhaltig kann mit Hilfe von Anwendungskontrolle die Ausführung von Schadprogrammen verhindert werden. Hierfür kann unter Windows AppLocker oder DeviceGuard eingesetzt werden.

Auch die Entkopplung von Browser und Arbeitsplatzcomputer (APC) mittels Remote-Controlled Browser System (ReCoBS) / Terminal-Server, Surf-VM, uvm. reduziert die Angriffsfläche deutlich.

5.1.3 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 von Ransomware durch eine Schadsoftware 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

5.1.4 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)

5.1.5 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 mit Rechten eines Nutzers wäre aber nicht mehr möglich. Wenn der Angreifer Admin- oder Domain-Admin-Rechte hat schützt diese Einschränkung kaum.

5.1.6 Netzwerke segmentieren

Eine saubere Netzsegmentierung hilf Schäden zu begrenzen, da die Ransomware damit nur die Systeme in unmittelbarer Nachbarschaft erreichen kann. Hierbei ist insbesondere auch die sichere Verwendung von Administrator Accounts (s.o.) notwendig , da ansonsten ein zentraler Bestandteil des Sicherheitskonzepts untergraben wird [19], [20].

5.1.7 Remote-Zugänge sichern

Wie bereits bei den Angriffsvektoren beschrieben, versuchen Angreifer 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. Auch müssen Sicherheitsprobleme zügig behoben werden. Auch müssen für Sicherheitslücken bereitgestellte Patches oder Workarounds zügig eingespielt werden, um einem Angriff von Außen zuvor zu kommen.

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

5.1.8 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 Administratoren normale Nutzerkonten. Dies sollte technisch 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. Für die Administration von Clients sollten keine Domänen-Administrationskonten verwendet werden.

5.1.9 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.

19 https://docs.microsoft.com/de-de/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material
20 https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/plan/forest-design-models

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.

5.2 Backups / Datensicherungskonzept

Ein Backup ist die wichtigste Schutzmaßnahme, mit der im Falle eines Ransomware-Vorfalls die Verfügbarkeit der Daten gewährleistet werden kann. Jede Institution sollte über ein Datensicherungskonzept (IT Grundschutz Kompendium: CON.3. Datensicherungskonzept) verfügen und dieses auch umsetzen.

Hierbei gibt es viele verschiedene Möglichkeiten für Backups, etwa mit Raid, in einer Cloud, mit NAS, etc... Es ist inzwischen bei Schadprogramm-Infektionen üblich, dass Angreifer mit zuvor erlangten Administrationsrechten gezielt nach allen Backups suchen und diese ebenso wie Produktivsysteme verschlüsseln.

Daher sollten die Daten in einem **Offline-Backup** gesichert werden. Diese Backups werden nach dem Backup von den anderen Systemen der Institution getrennt und sind daher von Remote-Angriffen geschützt. Offline-Backups können etwa mit getrennten Tapes, in einem getrennten Archiv mit nötigem physischem Zugriff oder auch in einem komplett vom eigenen Netz getrennten Cloud-Speicher erfolgen. Diese Backups sollen nicht regulär erreichbar (d.h. sollten in der Regel offline) und überschreibbar sein.

Zu einem Backup gehört auch immer die Planung und Vorbereitung des Wiederanlaufs und der Rücksicherung der Daten. Diese Planungen sollten auch einem Praxistest unterzogen werden, um Komplikationen und Herausforderungen in der Rücksicherung bereits vor einem Ernstfall zu erkennen.

5.3 Awareness / Schulungen / Mitarbeitersensibilisierung

Mögliche Themen in Awareness-Kampagnen und in der Schulung von Mitarbeitern sind insbesondere zwei ganz wesentliche Infektionswege für Schadprogramme:

- 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, wird nach dem Öffnen des maliziösen Anhangs 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. Alternativ wird der Besucher der maliziösen Webseite dazu ermuntert, eine gefährliche Datei herunterzuladen und zu öffnen. Dabei geben sich Angreifer beispielsweise auch als etablierte Cloud-Dienste aus oder greifen auf diese zurück, um Legitimität zu suggerieren. 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. 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 oder Geschäftspartnern empfiehlt sich ein Anruf. Bleiben Sie wachsam und vorsichtig.

Bitte beachten Sie, dass auch bei der besten Schulung der Mitarbeiter, die Erfolgsrate nur begrenzt ist. Schulungen sollten nie die einzige Schutzmaßnahme sein, es müssen immer auch noch technische und organisatorische Maßnahmen getroffen werden.

5.4 Weitergehende Schutzmechanismen

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

5.4.1 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 Windows Script Host (WSH)

5.4.2 PowerShell einschränken

Viele der aktuellen Malware-Exemplare sind auf PowerShell angewiesen, um ihr schadhaftes Potential entfalten zu können. Schränkt man die PowerShell entsprechend ein, ist eine Ausführung des eigentlichen Schadcodes oft nicht mehr möglich.
Da hier auch einige von Ihnen erwünschte Funktionen eingeschränkt werden könnten, sollten Sie zuvor testen, welche Einschränkungen sich hierdurch ergeben.

Der von Microsoft bereitgestellte „ConstrainedLanguage Mode“ erscheint daher als geeignet einen erhöhten Schutz vor PowerShell basierter Schadsoftware zu bieten.[21] [22]
Dieser wird wie folgt dauerhaft aktiviert:

Als Admin:
```
[Environment]::SetEnvironmentVariable('__PSLockdownPolicy','4'.'Machine')
```

Mit der Firewall kann der Internetzugriff für PowerShell blockiert werden. Dies schränkt viele Schadprogramme ein, wenn diese weitere Module oder Schadprogramme nachladen wollen.

Wenn Sie alle Netzwerkverbindungen für PowerShell blockieren möchten sieht dies z.B. wie folgt aus:

```
Powershell64 All Yes Block No %SystemRoot%\SysWOW64\WindowsPowerShell\
v1.0\powershell.exe Any Any Any Any Any Any Any Any Any

Powershell32 All Yes Block No %SystemRoot%\system32\WindowsPowerShell\
v1.0\powershell.exe Any Any Any Any Any Any Any Any Any
```

5.4.3 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[23].

5.4.4 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.

21 https://cert.at/de/blog/2019/11/201911-powershell-constrainedlanguage
22 https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_language_modes?view=powershell-6
23 https://www.heise.de/security/artikel/Erpressungs-Trojaner-wie-Locky-aussperren-3120956.html

Soweit Kapazitäten vorhanden sind sollten die Logs auch regelmäßig auf Auffälligkeiten überprüft werden. So gibt es Schadsoftware, welche versucht mittels Brute-Force sich auf die Netzwerklaufwerke zu verbinden und sich hierüber zu verbreiten. Dies kann bei aktivem Monitoring der Logs bereits in einem frühen Stadium erkannt werden und so weitere Schäden verhindert werden.

5.4.5 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 Projekt Abuse.Ch bietet Informationen zu aktiven C2-Servern, sowie auch zu kompromittierten Seiten, die Nutzer mit Ransomware infizieren[24].

5.4.6 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.

5.4.7 Planbesprechungen und Übungen

Übungen sind ein vielfältig einsetzbares Mittel. Schon einfache Planbesprechungen und 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 für ACS-Mitglieder auf der Webseite bereitgestellte Musterübung "Betroffen" mit geeigneten Anpassungen verwendet werden. Dies ist eine Planbesprechung, bei der Institutionen die eigenen Prozesse im Falle einer Ransomware-Infektion beüben können.

24 https://abuse.ch/

6 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 insbesondere bei einem Ransomware-Vorfall zu beachten sind.

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

Weitere Hinweise im Notfall finden Sie auch im Dokument „Erste Hilfe bei einem schweren IT-Sicherheitsvorfall“ welches auf der BSI-Webseite[25] oder auch direkt bei dem BSI auf Nachfrage erhalten können.

6.1 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 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 oder ausgeleitete Daten auch wirklich löschen.

6.2 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 schlussendlich verurteilt werden, damit keine weiteren Straftaten begangen werden können.

Das Bundeskriminalamt 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[26] zum Thema finden Sie auf den Webseiten der Allianz für Cybersicherheit.

Privatpersonen können bei der nächsten lokalen Polizeidienststelle Anzeige erstatten.

25 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf

26 https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Kontakt-zur-Polizei/kontakt-zur-polizei_node.html

6.3 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.

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. Teilweise kann eine bestehende Cyber-Versicherung hierbei auch helfen.

Das BSI arbeitet im Rahmen der Allianz für Cybersicherheit mit etablierten Unternehmen mit dem Schwerpunkt Computerforensik aus Deutschland zusammen. Auch hat das BSI eine Liste qualifizierter APT-Response-Dienstleister veröffentlicht[27]. Zusätzlich hat das BSI das Dokument „Erste Hilfe bei einem schweren IT-Sicherheitsvorfall“ veröffentlicht[28].

Opfer von Ransomware können auch im Forum der Botfrei Initiative Unterstützung erhalten. Dort beantworten Experten des Anti-Botnetz Beratungszentrums[29] Fragen von Betroffenen.

27 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf
28 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf
29 https://blog.botfrei.de/forums/

Wenn Sie Mitglied in einem Verband sind, können Sie ggf. auch von dieser Seite Unterstützung erhalten. Nutzen Sie Ihre Netzwerke und Beziehungen um ggf. Hilfen, Unterstützung, Personalverstärkung, Entlastung, Übernahme von Teilservices als temporäre Alternative, etc. zu erhalten.

7 Weitere Informationen

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

7.1 Produkte des BSI

7.1.1 Öffentlich

Pressemitteilungen:

- Fortschrittliche Angriffe – Dynamische Entwicklung:
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/Fortschrittliche-Angriffe/Fortschrittliche-Angriffe_node.html
- BSI warnt vor gezielten Ransomware-Angriffen auf Unternehmen:
  https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2019/BSI_warnt_vor_Ransomware-Angriffen-240419.html
- Jeder zweite von Datenverlust betroffen:
  https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2018/Umfrage_Back-up_26032018.html
- COVID-19 hat erhebliche Auswirkungen auf die IT-Sicherheitslage in Deutschland und Frankreich:
  https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/DF-Lagebild_171220.html

7.1.2 Bundesverwaltung, VerwaltungsCERTs, 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
- BSI Cyber-Sicherheits Vorfallsinformation
- BSI Themenlagebilder
- BSI Musterübungen

Hinweis: Jedes Unternehmen bzw. jede Institution in Deutschland kann über eine kostenlose Mitgliedschaft in der Allianz für Cyber-Sicherheit[30] Zugriff auf die genannten Dokumente erhalten.

7.2 Externe Informationen

7.2.1 Anti Botnetz Beratungszentrum

Das Anti Botnetz Beratungszentum stellt diverse Hilfen für Betroffene bereit:

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

https://www.botfrei.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

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/

8 Anlagen

8.1 Entwicklung von Ransomware

8.1.1 Phase I: Die Anfänge

Die Anfänge der Ransomware reichen bis ins Jahr 1998 zurück als die erste Ransomware, bekannt unter dem Namen AIDS-Trojaner oder PC Cyborg, auf 20000 Disketten verschickt wurde. Die Zahlung sollte damals noch auf ein normales Konto in Panama erfolgen. Einfacher wurde die Methode durch das starke Wachstum des Internet. Ab 2006 wurde dann die effektivere asymmetrische RSA-Verschlüsselung eingesetzt, zum Beispiele beim Trojaner Archiveus und GPcode. Ab 2011 begann eine exponentielle Wachstumsphase der Ransomware-Varianten. Bekannte Namen sind CryptoLocker (ab 2013), CryptoWall (ab 2014) oder TeslaCrypt (ab 2015), ab 2016 ist beispielsweise Locky sehr erfolgreich. Etwa ab 2013 wurde auch die Verwendung der Währung Bitcoin attraktiv für die Lösegeldzahlungen, da sie zunehmend als Zahlungsmittel Akzeptanz fand und eine erhöhte Anonymität gewährte[31].

8.1.2 Phase IIa: Effiziente Verbreitung und Zerstörung

Auch wenn es in den Jahren zuvor bereits technische Weiterentwicklungen gab, stellen die Jahre 2016 und 2017 ein Zäsur in der Entwicklung der Ransomware dar. 2016 gab es bereits eine Ransomware mit der Bezeichnung Petya, die neben der Verschlüsselung auch den Master-Boot-Record (MBR) der Festplatte überschrieb und damit das Betriebssystem von einem ordentlichen Neustart abhielt. 2017 kam dann mit WannaCry[32] die bis heute erfolgreichste Ransomware in Bezug auf ihre Verbreitung auf den Markt. Sie nutzte eine weit verbreitetet Schwachstelle (EternalBlue) im Betriebssystem Windows aus, um sich als Wurm auf alle von einem infizierten Rechner erreichbaren Windowssysteme zu verbreiten. Die epidemieartige Verbreitung war wochenlang in der Tagespresse und traf große Unternehmen im Transportwesen und in der Chemie. Selbst heute werden noch von einigen IT-Sicherheitsfirmen WannaCry-Infektionen als wichtiges Gefahrenpotential betrachtet, weil immer wieder aufs Neue veraltete, ungepachte Systeme erreicht werden können. Kurz nach Erscheinen von WannaCry wurde diese Art der Verbreitung in der Ransomware NotPetya mit einer schärferen Waffe kombiniert. Diese Software gab dem Opfer nämlich gar nicht erst die Möglichkeit, seine Daten wieder zu entschlüsseln, und muss daher als Werkzeug zur Sabotage angesehen werden. Die Absicht hinter WannaCry bleibt dagegen nebulös, da sich aufgrund er Zuordnung zur Nordkoreanischen Lazarusgruppe auch politische Ziele erahnen lassen[33].

8.1.3 Phase IIb: Professionalisierung

Etwa zur gleichen Zeit (ab 2016) wurde eine bereits länger bekannte Vorgehensweise weiterentwickelt und verbreitete sich im Bereich Ransomware. Sie bestand darin, dass der Entwickler der Software diese nicht direkt anwendet, sondern weiterverkauft. Außerdem wird dem Kunden die Dienstleistung zur Anpassung an die Umgebung der potentiellen Opfer und die Veränderungen der Forderungsnachrichten angeboten[34]. Dieses Konzept nennt sich Ransomware-as-a-Service, kurz RaaS. Wie in der restlichen Geschäftswelt auch gibt es dazu ausgefeilte Geschäftsmodelle, in denen minutiös der Anteil am erzielten Lösegeld geregelt ist.

31 https://www.it-daily.net/it-sicherheit/cyber-defence/11716-eine-kurze-geschichte-der-ransomware
32 https://entwickler.de/online/security/wannacry-ransomware-erklaert-579799880.html
33 https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks
34 https://ctb-benda.de/ksn-report-ransomware-in-den-jahren-2016-2017/

Ab 2017 zeichnet sich auch eine Fokussierung der Täter auf Unternehmen ab. Die bis dato üblichen für Privatpersonen zwar hohen, für Unternehmen aber nebensächlichen Lösegeldforderungen von einigen hundert bis einigen tausend Euro bezogen sich noch auf einzelne Rechner. Werden jedoch signifikante Teile eines Unternehmens lahmgelegt, so bedroht dies die Geschäftsfähigkeit des ganzen Unternehmens. Neben der Zahlung von Lösegeld fallen oft deutlich höhere Kosten für die Restaurierung der Systeme, Ausfallzeiten und die Erstellung eines neuen Sicherheitskonzeptes an. Daneben droht ein erheblicher Reputationsverlust. Für viele Unternehmen wird dies schnell existenzbedrohend, so dass die Bereitschaft steigt, stillschweigend höheren Lösegeldforderungen nachzukommen. Dieser Logik folgend, ging die Fokussierung auf Unternehmen und öffentliche Institutionen mit einer geänderten Taktik einher. Die Angreifer mussten mit der Ausspähung von Zugangsdaten, der lateralen Bewegung im Intranet und der Erschließung sämtlicher wertvoller Daten eher die Taktiken eines APT-Angreifers (APT = Advanced Persistent Threat) verwenden. Dieser Trend hat bis ins Jahr 2021 weiter Fahrt aufgenommen. Deshalb ist die Verhinderung dieses Vorgehens aus wesentlicher Bestandteil der weiter oben beschriebenen Maßnahmen.

8.1.4 Phase III: Modularisierung

Die neuesten Entwicklungen in der Ransomware-Branche zeigen, dass die Täter sich der ganzen Bandbreite ihrer Möglichkeiten bewusst sind und die bestehenden Geschäftsmodelle sich gegenseitig inspirieren. Dadurch ist eine Verschärfung bzw. Potenzierung der Gefahren einhergegangen. Waren in bisherigen Ransomware-as-a-Service-Angeboten[35] auch schon verschiedene Softwareanteile wie beispielsweise Exploit-Kits oder unterschiedliche kryptografische Algorithmen vereint, so hat diese Form der Modularisierung jetzt einen Großteil der Malware-Branche erreicht.

Emotet ist ein Beispiel für diese Entwicklung. Diese Schadsoftware begann ursprünglich als Bankingtrojaner. Die Funktionen von Emotet wurden aber mit der Zeit immer weiter ausgebaut. Neben „klassischen“ Malware-Binaries wird nun auch Ransomware nachgeladen. Emotet ist auch zum Spion für Zugangsdaten geworden und sammelt Mail-Adressen und Kommunikationsprofile der Opfer. In befallenen Unternehmen kundschaftet das Schadprogramm aktiv die Netzwerkumgebung aus und führt automatisierte Brute-Force-Methoden durch, um Zugangsdaten oder Access-Tokens der angemeldeten Nutzer zu erhalten. Mit diesen ist Emotet in der Lage sich lateral im Netzwerk auszubreiten und zu bewegen. Was Emotet nicht selbst erspähen kann, wird über nachgeladene Module wie Trickbot abgedeckt. So erhalten die Angreifer in großem Umfang Informationen über ein Opfer, wie Betriebsgeheimnisse oder Umsatzdaten, und können Lösegeldforderungen entsprechend maßschneidern[36]. Die Erpressung stellt allerdings nur den direkt sichtbaren Teil der Gefahren dar, die als "Triple Threat Attack" bezeichnet werden.

- Persönliche Kontaktdaten, Zugangsdaten und Schlüssel der betroffenen Nutzer sind kompromittiert.
- Informationen zu Bankverbindungen und Geldtransfers können abgeflossen sein.
- Betriebsgeheimnisse können für weitere Erpressungen oder Verkäufe an Interessenten verwendet werden.

Da sich die Module stetig weiterentwickeln und einer ebenso wachsenden Sammlung an Schwachstellen angepasst werden, stellt sich die davon ausgehende Bedrohung als exponentiell wachsend dar. Auch sind die hier beschriebenen Methodiken nicht auf Emotet und Trickbot beschränkt, sondern finden auch bei anderer Malware Anwendung.

35 Ransomware-as-a-Service lehnt sich an dem Modell Software-as-a-Service an und bedeutet, dass Angreifer die notwendige Infrastruktur und Schadsoftware wie eine Dienstleistung einkaufen. Die in diesem Kontext agierenden Dienstleister werden dann beispielsweise an den erpressten Lösegeldern beteiligt. Ransomware-as-a-Service ist das Modell des Cybercrime-as-a-Service übergeordnet, welches die unterschiedlichsten cyberkriminellen Dienstleistungen zusammenfasst.

36 https://www.security-insider.de/wie-emotet-zur-allzweckwaffe-wurde-a-798444/

8.1.5 Phase IV: Proliferation von Schadsoftware und Methoden

Im cyberkriminellen Umfeld hat das BSI festgestellt, dass sich Schadsoftware und Methoden zwischen Angreifergruppierungen ausbreiten. Insbesondere erfolgreiche Vorgehensweisen einer Angreifergruppe werden zeitnah auch von anderen Gruppen übernommen. Diese Verbreitung an cyberkriminellen Know-how und Technologien verfolgt das BSI als Proliferation von Schadsoftware und Methoden.

Die Veröffentlichung von Daten als weiteres Druckmittel in der Erpressung ihrer Opfer ist ein gutes Beispiel für diese Proliferation. Diese Methode wurde Ende 2019 von einigen wenigen Tätern eingeführt und im Laufe des Jahres 2020 entwickelte sie sich zum Standardvorgehen nahezu aller etablierten Cybercrime-Gruppen, die mit Ransomware ihre Opfer erpressen.

Diese Proliferation wird zusätzlich durch die bereits vorgenannte Modularisierung und Arbeitsteilung im Cybercrime-Umfeld begünstigt. Dieses Phänomen wird als übergeordneter Begriff auch zusammenfassend als „Cybercrime-as-a-Service“ (CCaaS; Cyberstraftat als Dienstleistung) bezeichnet.[37]

Jenseits der Verschlüsselung, Löschung und Veröffentlichung von Daten als Druckmittel in einer Erpressung hat das BSI bisher auch weitere Erpressungsmethoden festgestellt, die im Zusammenhang mit Ransomware-Vorfällen eingesetzt wurden:

- **Erregung öffentlicher Aufmerksamkeit bei Partnern und Kunden des Opfers**:
  - Einige Angreifer gehen aktiv auf Kunden und Partner oder auch die Öffentlichkeit zu, um zusätzlichen Druck auf einen Betroffenen auszuüben. Insbesondere bei einem intransparenten Umgang mit einem Vorfall kann dies langfristig den Ruf der Betroffenen schädigen.
- **Versteigerung bzw. Verkauf sensibler Daten (meist Alternativ zur Veröffentlichung)**:
  - Einige Angreifer versteigern bzw. verkaufen erbeutete Daten alternativ zum Veröffentlichen, sollte der Betroffene zu keiner Lösegeldzahlung bereit sein. Im Gegensatz zu einer Veröffentlichung auf einer Leak-Seite können die Angreifer so noch Profit aus den Daten generieren.
- **Androhen einer Meldung bei der zuständigen Datenschutz- o. Regulierungsbehörde:**
  - Im Zusammenhang mit einem Cyber-Angriff können vom Opfer Verstöße gegen die Datenschutz-Grundverordnung oder anderer regulierender Verordnungen begangen werden, wenn der Betroffene beispielsweise seiner Meldepflicht nicht nachkommt. Diese Verpflichtungen und daraus ggf. erwachsenden Strafen für den Betroffenen nutzten einige Angreifer als weiteres Druckmittel, in dem sie androhen, die Regulierungsbehörde über den Verstoß zu informieren.
- **Einsatz von DDoS-Angriffen in der Verhandlungsphase**:
  - Einzelne Angreifer setzten während der Verhandlung eines Lösegelds zusätzlich DDoS-Angriffe ein, um das Opfer weiter unter Druck zu setzen und die Ernsthaftigkeit der eigenen Aussagen zu unterstreichen.

Das BSI erwartet, dass cyberkriminelle Angreifer ihre Vorgehensweisen und Erpressungsmethoden weiterhin stetig ausbauen werden.

37 Cybercrime-as-a-Service hat das BKA im Bundeslagebild Cybercrime 2019 detailliert dargestellt. vgl. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2019.html

8.2 Ransomware in der Zukunft

8.2.1 Lokale Änderungen der Rahmenbedingungen für den IT-Betrieb

Die beschriebenen Bedrohungen sind bereits heute allgegenwärtig. Zukünftig werden allerdings weitere Herausforderungen auf Betreiber und Nutzer von IT-Systemen zukommen, von denen im Folgenden die wichtigsten beschrieben werden. Gerade bei kleinen und mittleren Unternehmen und Institutionen erfordern diese Herausforderungen erhöhte Aufmerksamkeit. Ransomware stellt dabei nur eine Bedrohung dar, die jedoch, wie die Beispiele zeigen, schnell fatale Folgen haben kann. Bei öffentlichen Einrichtungen können lange Ausfallzeiten und hohe Kosten entstehen. Für kleine und mittleren Unternehmen können vergleichbare Ausfälle in einer Insolvenz resultieren.

Internet of Things

Mit dem "Internet of Things" (IoT) wird bereits seit Jahren eine Vision beworben, die ein starkes Wachstum in verschiedenen Bereichen verspricht. Es geht um elektronische Geräte, die mehr oder weniger autonom Daten über das Internet austauschen. Viele dieser Geräte können auch über Smartphones oder Web-Anwendungen gesteuert oder konfiguriert werden. Der Trend geht dabei zu immer kleineren auch über lange Zeit autonom agierenden Einheiten, die unabhängig vom Stromnetz über Batterie oder Solar-Module betrieben werden.

LPWAN

Für die Kommunikation dieser Module werden momentan in vielen Ländern Infrastruktur-Techniken entwickelt, die sich unter dem Akronym LPWAN zusammenfassen lassen: Low Power Wide Area Network. Mit dieser Technik können Geräte mit einer Batterie bestückt über mehrere Jahre und mehrere Kilometer Entfernung ihre Daten an einen Empfänger senden.

Aufgrund der hohen Reichweite bei gleichzeitig niedrigem Stromverbrauch erschließen sich für diese Technologie viele Anwendungsgebiete, bei denen es um die Anbindung einfacher Sensorik an Orten ohne direkte Stromversorgung geht. Primär sind hier die Bereiche Logistik, Industrie, Smart City oder Smart Agriculture zu nennen. Den LPWAN-Markt beherrschen derzeit im Wesentlichen die vier unterschiedlichen Anbieter beziehungsweise Technologien Sigfox, LoRA, MIOTY, und NB IoT (LTE-M). Diese Techniken stehen unter hohem Konkurrenzdruck, da die Schätzungen für die Anzahl der im Jahr 2020 installierten IoT-Geräte zwischen 20 und 30 Milliarden Einheiten liegt[38] [39]. In der technischen Spezifikation bzw. Umsetzung dieser Technologien sind teilweise bereits Sicherheitslücken gefunden worden, teilweise auch in Folgeversionen geschlossen worden[38] [40]. Es ist zu erwarten, dass in diesen Techniken, der zugrundeliegenden Hardware oder individuellen Implementierungen auch in Zukunft Schwachstellen gefunden werden.

Aufgrund ihrer Eigenschaften stellt der Ausbau der eigenen IoT-Technik unter Verwendung der LPWAN-Techniken eine inhärente Gefahr dar:

- Die konkurrierenden Techniken werden den Markt nicht alle gleich abdecken und sich unterschiedlich entwickeln. Schwächere Markteilnehmer werden möglicherweise an der Sicherheit sparen oder vom Markt verschwinden, während die Geräte noch weiter betrieben werden. Dadurch wird sich die Zahl der unsicheren Geräte stark erhöhen und damit die generelle Angriffsfläche entsprechend steigen.
- Über LPWAN angebundene Geräte müssen sich nicht im direkten Zugriff von Mitarbeitern befinden und können daher u.U. dem physischen Zugriff von Angreifern ausgesetzt sein. Sie sind deshalb anfällig für Manipulationen, Austausch oder Man-in-the-Middle-Attacken.

38 https://www.mdpi.com/1999-5903/11/1/3/pdf
39 https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
40 https://fahrplan.events.ccc.de/congress/2018/Fahrplan/events/9491.html

- Einige der LPWAN-Techniken bieten auch Schnittstellen zu anderen Verbindungsarten (z.B. WLAN). Zusammen mit der räumlichen Verteilung könnten hier neue, noch nicht bekannte Angriffsszenarien entstehen.
- Da die einzelnen Einheiten u.U. sehr preiswert sind und entsprechend viele davon zum Einsatz kommen können, wird ihnen wahrscheinlich nicht die gleiche Aufmerksamkeit wie beispielsweise Arbeitsplatzrechnern gewidmet werden. Das Fehlen einzelner Geräte wird beispielsweise gar nicht wahrgenommen bzw. nicht mit entsprechender Priorität behandelt. Trotzdem kann je nach Gesamtarchitektur des Netzes jedes Gerät die Lücke im System darstellen.
- Neben der Verbindungstechnik sind weitere Komponenten zur Steuerung notwendig, z.B. Smartphone-Apps. Für kleinere Betriebe ist die Handhabbarkeit der Technik ausschlaggebend. Deshalb setzen sich spartenübergreifend Firmen durch, die bereits in anderen Gebieten Erfolg hatten und einfache, internetbasierte Lösung anbieten, die aber wesentlich wahrscheinlicher Sicherheitslücken aufweisen[41]. Bei der Abwägung zwischen Funktionalität und Sicherheit fällt oft gerade bei kleinen und mittleren Unternehmen und Institutionen die Entscheidung zugunsten der Funktionalität aus.

Cloud

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (Infrastructure-as-a-Service, IaaS), Plattformen (Plattform-as-a-Service, PaaS) und Software (Software-as-a-Service, SaaS).

So lassen sich etwa anfängliche Investitionen einsparen, die bereitgestellte Dienstleistung kann den individuellen Bedürfnissen dynamisch angepasst werden und Teile der Aspekte Sicherheit und Wartung können dem Dienstleister überlassen werden. Die Services sind über das Netz verfügbar und nicht an einen bestimmten Client gebunden. Die Ressourcen des Anbieters liegen in einem Pool vor, aus dem sich viele Anwender bedienen können. Dabei wissen die Anwender in der Regel nicht, wo die Ressourcen sich befinden und wer außer ihnen noch die Hardware nutzt. Die Separierung in der Cloud erfolgt häufig logisch, wo sie bei eigener IT noch physisch war.
Die Services können schnell und elastisch zur Verfügung gestellt werden, in manchen Fällen auch automatisch. Aus Anwendersicht scheinen die Ressourcen daher unendlich zu sein. Die Ressourcennutzung kann gemessen und überwacht werden und entsprechend bemessen auch den Cloud-Anwendern zur Verfügung gestellt werden.

Hierdurch ergeben sich eine Reihe von Chancen für den Umgang mit Ransomware:

- Wartung und Patchmanagement für gebuchte Services werden von einem professionellem Anbieter übernommen.
- Konsolidierung und Homogenität der bereitgestellten Ressourcen erlauben es dem Anbieter, Patches und Sicherheitsmechanismen in der Breite bereitzustellen (z. B. Gehärtete VM-Templates als Standard, IDS für alle Systeme durch den Provider).
- Erzielung eines hohen Grundniveaus an sicherer Infrastruktur, wenn große Teile durch einen professionellen Dienstleister realisiert werden (z. B. SaaS statt IaaS).
- Gerade Backupdienste mit Versionierung ermöglichen die Wiederherstellung unverschlüsselter Dokumente, sofern die Versionierung nicht über das Filesystem, und damit durch die Ransomware zugänglich ist.

Demgegenüber stehen durch die Zentralisierung bei einer externen Firma jedoch auch eine Reihe von Risiken in Bezug auf Ransomware:

41 https://media.ccc.de/v/35c3-9723-smart_home_-_smart_hack

- Systeme sind per se von außerhalb des eigenen Netzes zu erreichen und müssen entsprechend abgeschottet werden. Die Komplexität von Cloud-Infrastrukturen und die Vielzahl von Verwaltungsebenen erschweren das Erreichen dieses Ziels. Bisherige Sicherheitsvorfälle zeigen, dass Fehlkonfigurationen eine häufige Ursache für die Verwundbarkeit von Systemen darstellen.
- Öffentliche Schnittstellen (APIs) von Cloud Diensten sind einer kontinuierlichen Bedrohung aus dem Internet ausgesetzt. Angriffsversuche müssen daher detektiert und behandelt werden (logging, alerting).
- Die beim Anbieter eingesetzten Mandantentrennungsmechanismen müssen gewährleisten, dass sich Infektionen nicht über Mandanten hinweg ausbreiten. Im Kontext von Ransomware gilt dies v.a. für Storage-Komponenten und den Zugriff darauf.
- Das dynamische Allokieren von Ressourcen birgt die Gefahr, dass durch Malware verursachte Hochlast finanziellen Schaden verursacht.
- Die Infektion des Diensteanbieters und seiner Infrastruktur birgt das Risiko, dass in diesem Zuge auch Kundensysteme und -daten, sowie deren online durchgeführte Backups kompromittiert werden.

Durch die Nutzung von Cloud Computing verlagert sich auch die Bedrohung durch Ransomware. Die Auslagerung von IT kann die Sicherheit der eingesetzten Systeme verbessern, wenn ein professioneller Anbieter neben Bereitstellung der Ressourcen auch deren Pflege im Sinne von Patchmanagement und Wartung übernimmt. Gleichzeitig vergrößert sich durch die globale Erreichbarkeit und die Teilung von Ressourcen die Angriffsoberfläche der Infrastruktur. Die unter Kapitel 5 Präventionsmaßnahmen genannten Maßnahmen können daher auch beim Cloud Computing und der Verwendung externer IT angewandt werden.

Fehlende Fachkräfte

Ein wesentlicher Grund für die Bevorzugung von Cloud-Lösungen liegt in der Abgabe von Verantwortlichkeiten. Während es früher für kleine Unternehmen reichte, die Rollen und Rechte verschiedener Mitarbeiter vom Sekretariat zusammen mit der Mitarbeiterkartei pflegen zu lassen und allenfalls noch ein Datenbankadministrator zu benennen, sind bei der zunehmenden Digitalisierung inzwischen mehrere Experten für die Konzeption, Überwachung und Pflege der Informationstechnik notwendig. Eine Auslagerung an Dritte dazu noch preisgünstige Anbieter scheint daher logisch. Da sowohl Cloud-Anbieter als auch temporär beauftragte Dienstleister, die Speziallösungen anbieten, selten den Gesamtblick auf das Unternehmen oder die Institution haben, kann es sich trotzdem lohnen, Personal einzustellen, das alle sich ändernden Aspekte der digitalen Informationsverarbeitung im Betrieb im Überblick hat.

Leider sind die Fachkräfte, die solche Aufgaben übernehmen, selten verfügbar. Entweder sagen sie bei Bewerbungen erst gar nicht zu oder werden nach kurzer Zeit von anderen Unternehmen abgeworben. Große Unternehmen können in der Regel bessere Gehälter zahlen und bessere Aufstiegschancen in Aussicht stellen. Abgehende Mitarbeiter hinterlassen nicht selten undurchschaubare Strukturen und Werkzeuge, die ein Nachfolger ohne Einarbeitung kaum verwenden kann. Auch sind je nach Branche und eingesetzter IT-Hardware sehr unterschiedliche Kombinationen an Kenntnissen notwendig, die so nirgendwo ausgebildet werden.

Besitzt ein Unternehmen oder eine Institution also wichtige digitale Werte, die langfristig geschützt werden sollen, so sind in die Personalpolitik die Aspekte Sicherheit, Datenschutz und langfristige Begleitung der digitalen Informationsverarbeitung mit einzubeziehen und alle Optionen von eigenem Personal über zeitweilige oder kontinuierliche Dienstleister bis hin zum Einsatz von fertigen Cloud-Lösungen sorgsam abzuwägen.

Überforderung durch zunehmende Digitalisierung

Gerade kleinere Institutionen und Unternehmen sehen sich in Bezug auf die Digitalisierung verschiedenen Zwängen ausgesetzt. So fordern Mitarbeiter intern und Kunden von außen Dienstleistungen und Interaktionsmöglichkeiten, wie sie im freien Markt gerade Stand der Technik sind, auch wenn für eine adäquate Betreuung keine Kapazitäten zur Verfügung stehen. Auch in der öffentlichen Verwaltung werden in der Folge oft Schritte unternommen, deren Auswirkungen auf die Sicherheit der Daten und Prozesse nicht immer mit allen Konsequenzen durchdacht wurden.

Auf der anderen Seite herrscht auch eine zunehmende Erwartungshaltung von Politik und Gesellschaft, die eine Institution dazu drängt, Änderungen zu unternehmen, die im Nachhinein als Sicherheitsrisiko identifiziert werden. Hinzu kommt der schnelle Wandel in der Digitaltechnik. Sind beispielsweise Smartphones als Dienstgeräte eingeführt, kann sich gegen die zunehmende Sensorik, die zunehmende Zahl an Betriebssystemvarianten und Schwachstellen in den Anwendungen nicht mehr gewehrt werden. Der Trend zu vermischtem Gebrauch von privaten und dienstlichen Geräten, Stichwort "Bring your own device", erhöht die Angriffsfläche zusätzlich. Zudem kann ein einmal gemachter Schritt selbst dann nicht leicht zurückgenommen werden, wenn die Sicherheitsrisiken erkannt werden, weil die Abwägung zwischen den organisatorischen Vorteilen, der Bequemlichkeit und Zeitersparnissen gegen hypothetische Schadensfälle praktisch unmöglich ist.

Die zunehmende Zahl an Endgeräten, der autonomen Module (IoT), der Cloud-Dienste und der Kombinationsmöglichkeiten all dessen stellt eine enorme Vergrößerung der Angriffsfläche dar. Bei fehlendem Fachpersonal sind kleinere Institutionen daher oft überfordert, wenn es um die Sicherheit der gesamten digitalen Infrastruktur geht.

8.2.2 Internationale Entwicklungen

Neben der eingesetzten Hard- und Software, den organisatorischen und personellen Entscheidungen, die in einer Institution aktiv gewählt und beeinflusst werden können, sind bei der Ausgestaltung der Digitalisierung auch Faktoren zu berücksichtigen, die nicht in der eigenen Entscheidungsmacht liegen. Dies sind vor allem politische und wirtschaftliche Rahmenbedingungen, welche auch bei der Planung der IT-Sicherheit berücksichtigt werden sollten.

Deutschland als Ziel

Schon in der Vergangenheit haben deutsche Institutionen stark unter der Verbreitung von Ransomware gelitten. Trotzdem ist die Zahl der Fälle mit großen wirtschaftlichen Schäden noch vergleichsweise begrenzt. Die Gründe hierfür sind unklar und können von der Verfügbarkeit attraktiverer Cyberattacken wie z.B. Industriespionage bis zu der Tatsache reichen, dass Deutschland im Bereich der Digitalisierung, z.B. in der öffentlichen Verwaltung, nicht führend ist.

In jüngster Zeit nehmen Ransomwareattacken auf Gesundheitseinrichtungen oder öffentliche Verwaltungen aber auch in Deutschland zu. Gerade öffentliche Einrichtungen, deren Auftrag gesetzlich verankert ist, und alle Institutionen, die aus anderen Gründen unerlässlich also eine kritische Infrastruktur sind, stehen unter hohem Druck, Ausfälle ihrer Leistungen möglichst schnell zu beheben. Die Anzahl der Städte, die in den USA Opfer einer Ransomwareattacke geworden sind, ist erschreckend hoch und zeigt die Attraktivität dieser Ziele.

Diese Entwicklung muss aufmerksam beobachtet werden. Eigene Entscheidungen können auch davon abhängig gemacht werden, in welcher Weise eine gemeinsame Sicherung der IT-Landschaft in Zukunft auf Landes- oder Bundesebene vorgegeben wird.

Globalisierung

Während die Globalisierung in der Vergangenheit hauptsächlich dadurch auf die IT-Branche Einfluss nahm, dass durch die internationale Produktion die Preise gesenkt wurden und durch den weltweiten Absatz kürzere Produktzyklen möglich waren, sind die internationalen Verflechtungen durch die vermehrten Handelskriege und den weltweit steigenden Konkurrenzdruck zunehmend mit negativen Aspekten behaftet.

In Bezug auf die Verwundbarkeit allgemein bedeutet dies, dass in Deutschland geltende Standards für die IT-Sicherheit schwieriger durchgesetzt und kontrolliert werden können. Es gab bereits Vermutungen, dass in ausländischen Hardware-Komponenten Hintertüren für Kommunikationsmitschnitte oder Manipulationen eingebaut wurden. Selbst wenn diese Befürchtungen zweifelsfrei widerlegt werden könnten, können zukünftige Handelsbeschränkungen Einfluss auf die Tragfähigkeit heute getroffener Entscheidungen bzgl. Hard- oder Softwarebeschaffungen haben.

Politischer und wirtschaftlicher Druck / Funktionalität schlägt Sicherheit

Auch innerhalb von Deutschland besteht ein erheblicher Druck auf kleine und mittlere Unternehmen, Institutionen und regionale Behörden, Prozesse zu digitalisieren oder digitale Angebote zu ergänzen. Dieser wird teilweise auch von der Politik erzeugt. Nicht immer wird dabei die IT-Sicherheit ausreichend berücksichtigt. So gab es bereits politische Initiativen und rechtliche Vorgaben im Bereich der juristischen Verwaltung[42] und des Gesundheitswesens[43], die dazu führten, dass Anwendungen operativ verfügbar waren, obwohl sie erhebliche Sicherheitslücken besaßen. Bei kommunalen oder regionalen öffentlichen Dienstleistern spielen dagegen eher unscharfe Vorgaben für eine Modernisierung des Dienstleistungssektors eine Rolle.

Neben politischen Vorgaben kann aber auch der Vergleich mit anderen Unternehmen zu einem realen oder gefühlten Zwang werden, digitale Dienste anzubieten. So sind inzwischen viele mittelständische Unternehmen und sogar viele kleine Handwerksbetriebe gezwungen eigene Webseiten zu betreiben, um zumindest für Neukunden als Marktteilnehmer sichtbar zu werden. Wie weit solche Dienste getrieben werden, ist aber beeinflussbar. So ist etwa die Webseite mit Produkt-, Dienstleistungs- und Kontaktinformationen Standard. In wieweit allerdings ein Social-Media-Auftritt, Blog-, Kommentar- oder Chat-Funktionalitäten nötig sind, kann jede Institution selbst entscheiden.

Der Handlungsspielraum liegt dabei also einerseits in einer genauen Abwägung der benötigten Dienste. Andererseits sind politische Vorgaben nicht individuell umgehbar. Wenn daher Zweifel an der Sicherheit eingesetzter Hard- oder Software laut werden, sollten Initiativen zu Verschärfung der Sicherheitsanforderungen in den entsprechenden Verbänden gestartet werden, damit eine einzelne Institution sich keinem unverhältnismäßigem Sicherheitsrisiko aussetzen muss.

42 https://www.heise.de/newsticker/meldung/beA-Schwere-Panne-beim-besonderen-elektronischen-Anwaltspostfach-3927314.html
43 https://www.spiegel.de/netzwelt/apps/vivy-app-fuer-elektronische-gesundheitsakte-it-firma-findet-schwachstellen-a-1235854.html

8.3 Vorfälle

Für diese Fallsammlung wurden ausschließlich Informationen öffentlicher Quellen genutzt!

8.3.1 Auswahl internationaler Vorfälle

Betroffenheiten von staatlichen Verwaltungseinrichtigungen in den USA

Am 10. Mai 2019 veröffentlichte Recorded Future seine Studienergebnisse zu Ransomware-Vorfällen in staatlichen Einrichtungen. Sie konnten hierbei seit 2013 bis zur Veröffentlichung der Studienergebnisse 169 Vorfälle von Ransomware katalogisieren, wovon 21 Vorfälle aus den ersten Monaten des Jahres 2019 stammen[44]. Nach am 8. Oktober 2019 aktualisierten Zahlen stieg die Zahl für 2019 bereits auf 81 bestätigte Ransomware-Vorfälle in staatlichen Verwaltungseinrichtungen[45]. Exemplarisch wird nachfolgend auf drei Vorfälle eingegangen, die eine breite Beachtung in der Medienlandschaft hervorgerufen haben.

Atlanta von SamSam betroffen

Am 22. März 2018 stellten Mitarbeiter in der Stadtverwaltung von Atlanta fest, dass zentrale IT-Systeme und Dienstleistungen nicht mehr zur Verfügung standen. Ursächlich war eine Infektion mit der Ransomware SamSam. Nach Medienberichten waren durch die Verschlüsselung über ein Drittel aller 424 Software-Programme, welche die Stadt in unterschiedlichsten Bereichen einsetzte, von dem Angriff entweder direkt betroffen oder musste in der Folge offline genommen werden. 30% der betroffenen Programme wurden als geschäftskritisch identifiziert. Die Angreifer verlangten zur Entschlüsselung aller betroffenen Systeme $51.100 in Bitcoins. Die Stadtverwaltung lehnte eine Zahlung ab und kooperierte mit u. a. dem FBI für weiterführende Ermittlungen. Die Wiederherstellung der vollen Betriebsfähigkeit dauerte über Monate an. Der entstandene Schaden wurde noch nicht abschließend beziffert. Allerdings wurden von der zuständigen Behörde $9,5 Millionen zusätzliche Mittel zur Bewältigung der Folgen angefordert. Dieser Angriff gilt als einer der folgenreichsten Cyber-Angriffe gegen eine größere US-amerikanische Stadt[46].

Das US-Justizministerium hat am 26. November 2019 zwei Iraner als Entwickler und Anwender der Ransomware SamSam und damit auch als Angreifer hinter dem Angriff auf Atlanta angeklagt.[47]

Baltimore von RobinHood betroffen

Am 7. Mai 2019 stellte die Stadtverwaltung von Baltimore fest, dass zahlreiche ihrer IT-Systeme durch eine Ransomware verschlüsselt wurden. In der Folge waren u. a. zentrale Dienstleistungen wie das Zahlungswesen und das E-Mail-System eingeschränkt. Nach der Feststellung der Infektion wurden alle Systeme, die nicht für einen Notfallbetrieb notwendig sind, vom Netz getrennt oder abgeschaltet, um eine weitere Verbreitung der Ransomware zu unterbinden. Die Stadtverwaltung hatte das FBI für weitere Ermittlungen eingeschaltet. Nach Informationen der Zeitung *The Baltimore Sun* handelte es sich bei dem Vorfall um die Ransomware RobinHood[48]. Die Angreifer forderten 3 Bitcoins für die Entschlüsselung eines

44 https://www.recordedfuture.com/state-local-government-ransomware-attacks/
45 https://www.recordedfuture.com/state-local-government-ransomware-attacks-update/
46 https://www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1J231M
47 https://www.justice.gov/opa/press-release/file/1114741/download
48 https://www.baltimoresun.com/news/maryland/politics/bs-md-ci-it-outage-20190507-story.html

Systems oder 13 Bitcoins für die Entschlüsselung aller Systeme. Die Forderung belief sich zum Zeitpunkt der Erpressung entsprechend auf $17.000 für ein System oder $75.000 für alle Systeme.[49]

Nach Absprache mit dem FBI hat die Stadtverwaltung von Baltimore eine Zahlung des Lösegelds verweigert. Die Wiederherstellung der IT-Systeme und Wiederaufnahme der Dienstleistungen dauerte mehrere Wochen. Details über den Angriffsvektor sind nicht bekannt[50]. Die Kosten allein zur Wiederherstellung der verschlüsselten Daten soll sich für Baltimore nach Medienberichten auf bis zu $18 Millionen belaufen haben[51].

Texas von Sodinokibi (REvil) betroffen

Am Morgen des 16. Augusts 2019 wurden nach Informationen des föderalen Department of Information Research (DIR) 22 Kommunen des Bundesstaates Texas Ziel eines größer angelegten Cyberangriffs. Noch am selben Tag veröffentlichte das DIR eine Pressemitteilung über den Vorfall und informierte darüber, dass eine koordinierte Bewältigung des Vorfalls eingeleitet wurde[52].

Im Verlauf des Tages rief der texanische Gouverneur Greg Abott die zweithöchste Sicherheitsstufe des staatlichen Notfallsystems aus und klassifizierte den Vorfall damit als eine Gefahr, die zu groß ist, als das sich lokale Behörden der Sache ohne Unterstützung annehmen könnten. Erste Erkenntnisse der Behörden deuteten daraufhin, dass die 22 Kommunen von einem einzelnen Angreifer attackiert wurden[53].

Am 20. August gaben die Behörden weitere Informationen zu dem Vorfall bekannt, demnach sind grundlegende Dienstleistungen der kommunalen Verwaltungen betroffen wie Zahlungsabwicklungen und die Erstellung von Ausweisdokumenten. Darüber hinaus sind die Daten diverser Polizeiwachen sowie Bibliotheken ebenfalls verschlüsselt worden. Medienberichten zufolge soll der Angreifer eine Summe in Höhe von 2.5 Millionen USD verlangt haben, um die Systeme wieder zu entschlüsseln[54].

Nach Informationen des DIR wurde von den Opfern kein Lösegeld gezahlt. Aufgrund weiterführender Ermittlungen sind technische Details und Attributionen bzgl. des Angriffs derzeit noch nicht bekannt[55]. Dem Nachrichtenmagazin ZDNet zufolge soll vom Angreifer die Ransomware Sodinokibi, auch REvil genannt, zum Einsatz gekommen sein[56].

8.3.2 Auswahl verschiedener deutscher Vorfälle

Dem BSI sind eine Vielzahl an Fällen in Deutschland bekannt, bei denen es zu einer Infektion mit einer Ransomware kam. In Einzelfällen liegen die entstandenen Schäden nach ersten Einschätzungen der Betroffenen bei Beträgen bis in die Millionen Euro. Aufgrund laufender Ermittlungen der Strafverfolgungsbehörden und schutzwürdiger Interessen der Betroffenen können zu diesen Fällen von Seiten des BSI keine weiteren Aussagen getroffen werden.

Die nachfolgende Auswahl an Vorfällen hat eine breite Medienberichterstattung erwirkt und wurde von den Betroffenen gegenüber der Öffentlichkeit transparent kommuniziert.

49 https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html
50 https://arstechnica.com/information-technology/2019/05/baltimore-ransomware-nightmare-could-last-weeks-more-with-big-consequences/
51 https://www.newsweek.com/texas-ransomware-bitcoin-hackers-1454865
52 https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=206
53 https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=211
54 https://www.bleepingcomputer.com/news/security/hackers-want-25-million-ransom-for-texas-ransomware-attacks/
55 https://dir.texas.gov/View-About-DIR/Article-Detail.aspx?id=213
56 https://www.zdnet.com/article/at-least-20-texas-local-governments-hit-in-coordinated-ransomware-attack/

Dettelbach von TeslaCrypt betroffen

Am 8. März 2016 kam auf einem Arbeitsplatzrechner der Stadtverwaltung von Dettelbach die Schadsoftware TeslaCrypt zur Ausführung. In der Folge wurden Daten der Stadtverwaltung und der Stadtwerke verschlüsselt und ein Lösegeld in Höhe von 1,3 Bitcoin, damals ca. 490€, gefordert. Der Betrieb des Bürgerbüros wurde eingestellt. Im Netz der Stadtwerke wurden u. a. Jahresabrechnungen durch die Schadsoftware verschlüsselt. Um die Dienstleistungen der Stadt zügig wiederherzustellen, entschied sich die Stadtverwaltung dazu, die Lösegeldsumme über ein Fachunternehmen zu zahlen. Eine Entschlüsselung aller Daten war jedoch auch nach der Zahlung des Lösegelds nicht möglich. Hinzu kamen Fehler in der IT-Infrastruktur, die nicht unmittelbar mit der Schadsoftware zusammenhingen, welche die Wiederherstellung der Serviceleistungen erschwerte. Die vollständige Wiederherstellung der Betriebsfähigkeit dauerte mehrere Wochen an. Einige Bereiche, wie das Bürgerbüro, konnten allerdings bereits in der darauffolgenden Woche ihre Arbeit wiederaufnehmen. Die Stadtverwaltung hatte eine Anzeige gestellt. Ermittlungen wurden damals von den zuständigen Landesbehörden aufgenommen. Nach Medienberichten könnte der entstandene Schaden 100.000€ übersteigen[57] [58].

Staatstheater und Messe Stuttgart

Anfang April 2019 sind das Staatstheater und die Messe Stuttgart Opfer eines Ransomware-Angriffs geworden. Das zuständige Landeskriminalamt Baden-Württemberg ermittelte[59].
Der Angriff auf das Staatstheater erfolgte offenbar über eine IT-Firma, welche Fernwartungszugänge auf Systeme des Staatstheaters hatte[60]. Infolgedessen waren E-Mail und der Online-Ticketverkauf etwa fünf Tage nicht mehr nutzbar.
Bei der Messe Stuttgart waren infolge der Verschlüsselung Teile der Kommunikationsnetze gestört bzw. wurden aus Sicherheitsgründen deaktiviert[61]. Offenbar waren auch Tochterfirmen der Stadt Stuttgart wir die Stadtwerke, ein Eventpartner und das Marketingunternehmen der Stadt betroffen[62].

DRK Trägergesellschaft Süd-West

Der regionale Dachverband eines deutschlandweit aktiven Wohlfahrtsverbandes wurde in der Nacht des Wochenendes 13./14. Juli 2019 Opfer eines Ransomwareangriffs. Der Dachverband ist als zentraler IT-Dienstleister für seine Einrichtungen (Krankenhäuser, Gästehäuser, Gastronomie, angeschlossene Arztpraxen, etc.) aktiv. In der Folge mussten über 20 Gesundheitseinrichtungen, darunter mehrere Krankenhäuser, in Rheinland-Pfalz und im Saarland ihren IT-Betrieb einstellen und Notfallpläne aktivieren.

Der Angriff wurde am Sonntagmorgen, 14. Juli 2019, bemerkt. Die Schadsoftware habe Server und Datenbanken verschlüsselt. Dieser Verschlüsselungsvorgang wurde am Sonntagnachmittag gestoppt, wie die Trägergesellschaft mitteilte. Aus Sicherheitsgründen wurden schnell alle Server vom Netz genommen, um sie auf eine Betroffenheit zu überprüfen.
Die Notfallkonzepte zur sicheren Überbrückung des Ausfalls funktionierten.

57 https://www.spiegel.de/netzwelt/web/ransomware-teslacrypt-stadtverwaltung-dettelbach-zahlt-loesegeld-a-1080528.html
58 https://www.br.de/nachricht/unterfranken/inhalt/trojaner-angriff-dettelbach-reaktion-stadt-100.html
59 https://www.zvw.de/inhalt.cyberangriff-auf-messe-stuttgart-weitere-firmen-betroffen.e60c8fb3-b1af-441d-8048-9da701156abe.html
60 https://www.rnz.de/politik/suedwest_artikel,-stuttgarter-staatstheater-hacker-griffen-ueber-it-firma-an-_arid,432947.html
61 https://www.welt.de/regionales/baden-wuerttemberg/article199661746/Cyberangriff-auf-Messe-Stuttgart.html
62 https://www.sueddeutsche.de/service/internet-stuttgart-stuttgarter-firmen-nach-hackerangriff-wieder-erreichbar-dpa.urn-newsml-dpa-com-20090101-190909-99-806310

Die Krankenhäuser konnten durch die umgehende Aktivierung des internen Notfallbetriebs die medizinische Versorgung der Bevölkerung aufrechterhalten. Einzelne Fachverfahren waren eingeschränkt. Die medizinische Versorgung der Patienten war stets gewährleistet, wichtige Geräte nicht betroffen.

Es ermittelte die Landeszentralstelle Cybercrime bei der Generalstaatsanwaltschaft Koblenz. Die Ransomware wurde als „Sodinokibi“ (auch „REvil“ oder „Sodin“ genannt) identifiziert.

Die Bereinigungsarbeiten waren auch nach drei Wochen noch nicht abgeschlossen.

Quellen:[63],[64],[65],[66]

Neustadt am Rübenberge

Am Freitag den 6. September 2019 entdeckte das Personal der IT-Verwaltung Neustadt, laut einem Beitrag auf der städtischen Webseite, dass die örtlichen Systeme kompromittiert wurden. Um eine weitere Ausbreitung der Infektion zu verhindern, setzten die Zuständigen die Server vorerst außer Betrieb.

Einem Heise-Bericht zufolge handelt es sich bei der Schadsoftware um den Trojaner Emotet. Bei der Attacke auf Neustadt haben die Angreifer eine Ransomware nachgeladen, die offenbar sowohl Rechner, Server als auch Backups verschlüsselt hat.

Der Angriff hat große Teile der örtlichen Verwaltung außer Kraft gesetzt. Laut einer Stadt-Sprecherin haben Behörden kurz nach dem Angriff nur für telefonische oder mündliche Beratungen geöffnet, die Zulassungsstelle für Kraftfahrzeuge bleibt ganz geschlossen. Auch ist es laut einer Meldung des NDR zeitweise nicht möglich, Personalausweise oder Reisepässe zu beantragen. Die wichtigsten Datenbanken wie zum Beispiel Finanzen und Personal sind nicht verschlüsselt und können voraussichtlich wiederhergestellt werden.

10 Tage nach der ersten Verschlüsselung, war das Stadtbüro weiterhin nur eingeschränkt einsatzfähig. So war etwa das Ratsinformationssystem nicht aktualisierbar. Die Rechner der Mitarbeiter waren zu diesem Zeitpunkt wiederaufgesetzt, hatten aber noch nicht alle die benötigte Software, so dass die Bevölkerung gebeten werden musste, vor Geschäftsgängen telefonisch zu erfragen, ob die Dienstleistung erbracht werden kann. Die Stadtbibliothek blieb einen Monat nach Beginn der Verschlüsselung geschlossen. Hierfür wurden Ersatzdienste genannt. Die Telefonzentrale funktionierte nur eingeschränkt.

Quellen: [67],[68],[69],[70]

63 https://www.drk-khg.de/
64 https://www.siegener-zeitung.de/kirchen/c-lokales/massive-cyber-attacke-auf-krankenhaeuser_a177760
65 https://www.spiegel.de/netzwelt/web/rheinland-pfalz-und-saarland-hackerangriff-auf-krankenhaeuser-a-1277759.html
66 https://www.sueddeutsche.de/digital/ransomware-service-sodinokibi-1.4554518
67 https://www.ndr.de/nachrichten/niedersachsen/hannover_weser-leinegebiet/Trojaner-Neustadt-bleibt-bis-Freitag-offline,neustadt332.html
68 https://www.heise.de/security/meldung/Ransomware-Neue-Emotet-Welle-legt-Neustaedter-Stadtverwaltung-lahm-4518819.html
69 https://www.egovernment-computing.de/update-eine-stadt-geht-offline-a-863498/
70 https://www.haz.de/Umland/Neustadt/Neustadt-Behoerden-bleiben-nach-Virenangriff-die-ganze-Woche-geschlossen