Empfehlungen zu Ransomware

25. 3. 2016

Zusammenfassung

In den letzten Monaten ist die Gefährdung durch Ransomware deutlich gestiegen. Mehrere Gruppen von Angreifern kompromittieren die PCs ihrer Opfer, verschlüsseln dort die Dateien und verlangen Geld für die Wiederherstellung der Daten.

Wenn man unvorbereitet Opfer einer Ransomware geworden ist, gibt es keine wirklich guten Handlungsoptionen mehr. Es ist technisch fast nicht mehr möglich, seine Daten ohne Hilfe der Angreifer wiederherzustellen.

Daher sind die einzigen wirksamen Maßnahmen gegen Ransomware proaktiv: Regelmäßige, gut implementierte Sicherheitskopien reduzieren den möglichen Schaden und diverse Vorkehrungen können die Wahrscheinlichkeit eines Vorfalls deutlich reduzieren.

Es gibt kein Patentrezept gegen Ransomware. Auch gibt es wenig Hoffnung, dass diese Bedrohung in absehbarer Zeit verschwinden wird. Jeder Betreiber von Computern, vom privaten Heim-PC bis hin zu großen Firmennetzen sollte sich daher dieser Gefahr bewusstwerden und entsprechende Maßnahmen treffen.

Dieses Dokument gibt dazu Hintergrundinformation und konkrete Handlungsvorschläge.

Autoren:

Otmar Lendl <lendl@cert.at>
Christian Wojner <wojner@cert.at>

Danksagung:

Dieses Dokument enthält Ideen und Erfahrungswerte aus dem österreichischen CERT-Verbund und dem inneren Kreis der operativen Koordinierungsstruktur.

Feedback:

Kommentare oder Rückfragen bitte an team@cert.at.

Inhalt

Kontext

Wie jede andere Sphäre der Gesellschaft wird auch das Internet für kriminelle Aktivitäten genutzt. In vielen Fällen ist das Internet nur ein Werkzeug (analog zum Fluchtfahrzeug eines Bankräubers), Cybercrime im engeren Sinn[1] macht nur einen Teil davon aus.

Betrachtet man die Cybercrime Szene genauer, kann man feststellen, dass Angreifer oft keinerlei Probleme haben, PCs zu infizieren oder in Webseiten einzubrechen. Der Flaschenhals für die Kriminellen ist üblicherweise das Cash-out: wie machen sie aus den kompromittierten Systemen Geld, über das sie frei – und ohne Spuren zu hinterlassen – verfügen können.

„Ransomware“[2] ist eine Methode dafür. Sie basiert darauf, den PC oder die Daten des Opfers als „Geisel“ zu nehmen, und den Datenverlust als Druckmittel für die Forderung von Lösegeld zu nutzen.

Diese Methode ist nicht neu, sondern mindestens seit 2005[3] bekannt. „Ransomware“ ist der generische Begriff für eine Klasse von Schadsoftware, Beispiele sind etwa „GPcode“, der „BKA-Trojaner (Reveton)“, „CryptoLocker“, „CTB-Locker“, „TorrentLocker“, „Cryptowall“, „Locky“, „KeRanger“ oder „TeslaCrypt“.

Heute ist klar, dass das Geschäftsmodell hinter Ransomware nicht nur von einer einzelnen Gruppe von Angreifern umgesetzt wird. Es existieren bereits diverse Implementationen der Grundidee, welche in Form von Bausätzen verkauft werden. Auch die nötige Infrastruktur zum Betrieb einer Kampagne (inkl. der Server, die zur Ermöglichung der Entschlüsselung nach der Bezahlung nötig sind) kann heute zugekauft werden. Zusätzlich findet die schon bei Spam beobachtete Arbeitsteilung mittels „Affiliate“-Programmen[4] Anwendung.

Es gibt bisher keine gesicherten Zahlen über den von Ransomware verursachten Schaden bzw. die Profite der Kriminellen. Angesichts der Verbreitung scheint es sich um ein lohnendes Geschäftsmodell zu handeln – so hat etwa die Gruppe rund um Dridex den Schwenk von Online-Banking-Betrug hin zu Ransomware (Locky) gemacht. Die Analyse eines Sicherheitsforschers[5] ergab, dass eine CryptoWall Kampagne mehr als 300 Millionen USD eingebracht haben könnte. Genaue Zahlen für Österreich liegen uns nicht vor; IKARUS erwähnt in ihrem Security-Blog[6] „bis zu 200 Outbreaks täglich mit neuester Ransomware“.

Angesichts dessen ist davon auszugehen, dass das Thema Ransomware noch länger eine akute Bedrohung bleiben wird.

Die meisten Angriffe richten sich gegen Microsoft Windows PCs/Laptops, es wurden aber auch bereits Kampagnen gegen Windows Server, Apple MacOS X und Webserver unter Linux beobachtet. Dieses Dokument konzentriert sich auf die Gefährdung von Windows Clients.

---

[1] https://de.wikipedia.org/wiki/Computerkriminalit%C3%A4t
[2] https://de.wikipedia.org/wiki/Ransomware
[3] https://en.wikipedia.org/wiki/Ransomware
[4] http://www.npr.org/sections/alltechconsidered/2014/11/18/364730954/how-a-feud-between-two-russian-companies-fueled-a-spam-nation
[5] http://www.slideshare.net/cfbeek72/theres-a-pot-of-bitcoins-behind-the-ransomware-rainbow
[6] http://www.ikarussecurity.com/at/ueber-ikarus/security-blog/outbreak-warnung-cyber-attacken-auf-oesterreich/

Vorgehen der Angreifer

Da die Bedrohung durch Ransomware nicht nur von einer einzelnen Gruppe von Angreifern ausgeht, gibt es auch keine Vorgehensweise, die auf alle Fälle zutrifft. Die Erfahrungen der letzten Zeit haben gezeigt, dass es durchaus mehrere Szenarien gibt.

Initialer Einbruch

Am Beginn jedes Ransomware-Falles steht das Einbringen und das Ausführen eines Stücks Software in der Infrastruktur des Opfers. Typischerweise ist das nicht die eigentliche Ransomware, sondern nur ein kleiner Brückenkopf, der dann das Verschlüsselungsprogramm nachlädt.

Für diese initiale Codeausführung können verschiedene Vektoren benutzt werden. Aktuell werden folgende Methoden beobachtet:

Massenemail (Spam)

In diesem Fall verschicken die Angreifer (meist über Botnetze) Emails breit gestreut an potentielle Opfer. Enthalten ist eine Nachricht (Köder), die mittels Social Engineering den Empfänger dazu bringen soll, den Anhang zu öffnen und so zur Ausführung zu bringen.

Als Köder werden ähnliche Betreffzeilen benutzt, wie sie in den letzten Jahren schon für die Verbreitung von anderer Malware genutzt wurden. Dazu gehören unter anderem:

- Nachrichten von Paketdiensten
- Rechnungen
- Anwaltsbriefe / Drohungen
- Nachrichten von Social Networks

Als Dateianhänge wurden folgende Formate beobachtet:

- .exe Dateien
- Microsoft Office Dateien (.doc, .xls, .rtf, .docm, .xlsm, …) mit eingebetteten Macros
- JavaScript Dateien (.js)
- PDF mit eingebettetem ActionScript
- teilweise sind sie auch in (verschlüsselten) ZIP-Dateien verpackt
- …

In den meisten Fällen wird hier keine Schwachstelle ausgenutzt, um die Codeausführung zu erreichen, sondern es wird der Empfänger dazu gebracht, die Datei bzw. die eingebetteten Macros auszuführen.

Exploit Packs

Eine andere Strategie der Angreifer ist es, in möglichst viele Webseiten Code (ein sogenanntes „Exploit Pack“) einzubetten, der den Browser der Besucher angreift. Sind der Browser oder eine Erweiterung des Browsers (Java, Flash, PDF, …) veraltet, so werden Schwachstellen ausgenützt, um eine Codeausführung zu erreichen.

Es ist dokumentiert, dass Ransomware unter anderem von den Exploit Packs „Angler“, „Neutrino“, „Nuclear“, „Magnitude“ und „Rig“ verteilt wurde.

Eine großflächige Installation von Exploit Packs gelingt den Angreifern typischerweise entweder durch das Ausnutzen von Schwachstellen in verbreiteten (und oft schlecht gewarteten) Content Management Systemen (Wordpress, Joomla!, TYPO3, …), oder durch einen Einbruch in Verteilsysteme von Online-Werbung.

Angriffe auf Server

Neben den Angriffen auf Clients wurden auch folgende andere Angriffsmuster beobachtet:

1. Einbrüche in Webserver mit anschließender Verschlüsselung der Webinhalte
2. Einbrüche über Fernwartungszugänge (RDP, TeamViewer, …)
3. Einbrüche über Java-Schwachstellen (unsicheres JNI, veraltetes JBoss, …)

Nachladen der eigentlichen Ransomware

Im nächsten Schritt des Infektionsprozesses wird vom initial eingebrachten Code das (größere) Programm nachgeladen, welches in Folge erst die volle Funktionalität der Ransomware implementiert.

Kommunikation mit einem Command & Control Server

Wie die Ransomware die Parameter für die Verschlüsselung generiert, ob diese an einen von den Angreifern kontrollierten Server übermittelt werden, oder ob das Entschlüsseln der Daten (nach Bezahlung) keine vorhergehende Kommunikation der Ransomware mit den Angreifern voraussetzt, variiert zwischen den verschiedenen Implementationen. Der Trend scheint in die Richtung zu gehen, dass die Ransomware mit dem Command & Control Server kommuniziert, bevor sie mit der Verschlüsselung beginnt. So verbessern die Angreifer die Chance, dass eine Entschlüsselung möglich ist.

Bei manchen Versionen von Ransomware kann diese Kommunikation zur Erkennung einer Infektion verwendet werden.

Defensive Maßnahmen

Wie viele andere Schadsoftware setzt auch Ransomware Maßnahmen, die ihre Effektivität und ihre Persistenz erhöhen sollen. Die Details variieren je nach Variante, beobachtet wurden u.A.:

- Zeit verstreichen lassen, damit Analysewerkzeuge den Zweck der Software nicht sofort erkennen
- Erkennung von Merkmalen, die auf Analysesysteme (Reverse Engineering Software, Sandboxes, …) hindeuten
- Löschen von „Volume Shadow Copies“, die eine Rückkehr auf den Stand der Dateien vor der Verschlüsselung möglich machen würden
- Persistenz: der Verschlüsselungsprozess soll weiterlaufen, auch wenn der PC inzwischen neu gestartet wurde
- Verschleierung der unvollständigen Verschlüsselung: diese soll möglichst auf einen Schlag wirksam werden
- Deaktivieren von Antivirensoftware und Microsoft Windows Update

Verschlüsselung

Aktuelle Ransomware verschlüsselt Dateien auf der lokalen Festplatte, auf angesteckten Medien (USB-Sticks, Wechselplatten, …) und auf allen verfügbaren Netzwerklaufwerken. Die Kriterien, welche Dateien betroffen sind, variieren. In manchen Fällen ändert sich nach der Verschlüsselung der Dateiname und der Zeitstempel, in anderen Fällen erkennt man die Modifikation erst, wenn versucht wird die Datei zu öffnen.

Die Qualität der von Ransomware implementierten Verschlüsselung ist in den letzten Jahren deutlich besser geworden. War es früher immer wieder möglich, eine Hintertür zu finden und so die Datenrettung ohne Mithilfe der Erpresser zu schaffen, so ist das heute bei der gängigen Ransomware seltener möglich. Sie bedient sich inzwischen gut erforschter und getesteter kryptographischer Algorithmen.

Pro Opfer wird ein Schlüssel erzeugt, mit dem die Dateien mit einem symmetrischen Algorithmus (typischerweise AES) verschlüsselt werden. Oft wird eine Dateiendung angehängt, damit beim Öffnen die Meldung des Erpressers mit der Zahlungsaufforderung angezeigt wird.

Nach erfolgter Verschlüsselung will die Ransomware sicherstellen, dass dieser Schlüssel erst nach erfolgter Zahlung für das Opfer verfügbar wird. Wie das umgesetzt wird, variiert: er könnte per Netzwerkverbindung an die Angreifer übermittelt worden sein, oder er wird mittels asymmetrischer Kryptographie (etwa RSA) mit dem öffentlichen Schlüssel der Angreifer verschlüsselt. Auch andere Methoden, etwa komplexere Schlüsselableitungsfunktionen wie ECDH, wurden schon beobachtet.

Generell gilt, dass verschiedene Gruppen (bzw. Ransomware-Versionen) diverse Verfahren implementiert haben. Diese unterliegen einem Selektionsprozess, und nur die Methoden werden behalten, die sich (aus Sicht der Angreifer) bewährt haben.

Gegenmaßnahmen

Der vorangehende Abschnitt hat gezeigt, dass eine für die Angreifer erfolgreiche Ransomware-Infektion ein mehrstufiger Prozess ist. Die folgende, systematische Betrachtung der Gegenmaßnahmen nimmt diesen Prozess und baut darauf auf.

Es gibt keine Wunderwaffe gegen Ransomware, daher ist es wichtig, mehrstufige und einander ergänzende Maßnahmen zu setzen. Welche konkret am besten sind, hängt stark von den jeweiligen Gegebenheiten ab.

Nur wenige der hier vorgeschlagenen Maßnahmen richten sich speziell gegen Ransomware. Viele sind generische Empfehlungen zur Erhöhung der IT-Sicherheit. Dieses Dokument ist kein Ersatz für ausgereifte IT-Sicherheitsstrategien für Unternehmen (ISO/IEC 27000 Familie[7], Österreichisches Informationssicherheitshandbuch[8], BSI Grundschutz[9], …)

[7] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66435
[8] https://www.sicherheitshandbuch.gv.at/
[9] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Proaktiver Schutz

Wenn die initiale Codeausführung verhindert wird, dann lassen sich Ransomware-Angriffe verhindern. Folgende Strategien können dabei helfen:

- **Sicherheitsbewusstsein der User**

  In vielen Fällen braucht ein Angreifer die aktive Mithilfe des Opfers. Ein Attachment in einer Email welche ungelesen gelöscht wird, richtet keinen Schaden an. Wenn sich beispielsweise ein Benutzer nicht zur Aktivierung von Macros in Word überreden lässt, dann bleibt in diesem Fall die Infektion aus.

  Es macht daher für Organisationen Sinn, ihre Mitarbeiter auf die Gefahren hinzuweisen und sie im richtigen – und sicheren – Umgang mit Email zu schulen.

  Damit Nutzer Dateitypen klar erkennen können, empfiehlt es sich, Dateiendungen immer anzeigen zu lassen.

- **Effektive Filterung von Emails**

  Im besten Fall werden Emails mit gefährlichem Inhalt erst gar nicht zugestellt, sondern bereits im Vorfeld aussortiert. Dazu bieten sich etwa folgende Methoden an:

  - Spamfilterung

    Gute Spamfilter können viele Mails, die Ransomware enthalten, ausfiltern. Uns liegen auch Berichte vor, nach denen es Sinn macht, die häufig als Köder benutzten Betreff-Zeilen als Filterkriterium zu nutzen.

  - Filterung nach Dateityp

    Auch die Endungen der Anhänge in den Spam-Mails mit Ransomware eignen sich als Filterkriterium. Folgende Dateitypen können gefährlich sein und werden selten für legitime Zwecke in Emails verwendet: .exe, .cab, .bat, .cmd, .js, .vbs, .wsf, .msi, .scr, .chm, … In vielen Fällen werden diese Dateien in ein Containerformat (etwa ZIP) gepackt. Diese sollten vom Mailfilter entsprechend auf den Inhalt geprüft werden. Es gibt auch Kampagnen, bei denen das ZIP-File mit einem Kennwort versehen war, das im Text des Mails mitgeschickt wird. Wir empfehlen daher, verschlüsselte ZIP-Files möglichst nicht direkt im Postfach zuzustellen.

  - Klassische AV-Mailfilter

    Musterbasierte Virenscanner erreichen bei den aktuellen Ransomware-Spamwellen oft keine hohen Erkennungsraten – trotzdem sollte man auf sie nicht verzichten.

- Sandbox-basierte Filter

  Diese Klasse von Sicherheitslösungen öffnet den Mailanhang in einer virtuellen Umgebung und kann daher dessen Verhalten analysieren. Diese Produkte erreichen oft eine bessere Erkennungsrate als klassische AV-Mailfilter.

- **Schutz des Browsers**

  Um Webbrowser vor Exploit-Packs zu schützen sind folgende Punkte wichtig:

  - Alle relevante Software muss laufend und zeitnah auf den neuesten Stand gebracht werden: Browser, Erweiterungen (Java, PDF, Flash, …), Office-Pakete, Betriebssysteme.
  - Verkleinerung der Angriffsfläche: eine nicht installierte Software kann auch nicht missbraucht werden. So etwa sind Flash und Java für normales Surfen im Internet kaum mehr notwendig.
  - Sollte ein vollständiger Verzicht auf Browser-Erweiterungen nicht machbar sein, kann eine zusätzliche Benutzerinteraktion mittels einer „Click-to-Play“ Funktion ein guter Kompromiss sein.
  - Da auch Werbeplattformen gelegentlich zur Verteilung von Schadsoftware missbraucht werden, kann ein Einsatz von Werbeblockern hilfreich sein.

- **Einstellungen bzgl. Macros / Scriptsprachen**

  Macros in Office-Dokumenten (inklusive .rtf) und lokal gestartete JavaScript Files (.js) haben die gleichen Rechte wie .exe Dateien und sollten daher nur von vertrauenswürdigen Quellen angenommen und ausgeführt werden.

  Bei Office 2016 kann man etwa unter „Datei / Optionen / Trust Center“ einstellen, dass Macros gar nicht, oder erst nach Nachfrage, ausgeführt werden. Die optimalen Einstellungen zum Umgang mit Macros hängen hier stark von den lokalen Gegebenheiten ab.

  Auch der Windows Scripting Host und die Windows PowerShell können leicht bei einem unvorsichtigen Doppelklick zum Download von Schadsoftware benutzt werden. Beides kann deaktiviert werden; hier sollte vorher entsprechend getestet werden.

Verhinderung der Verschlüsselung

Das Nachladen und Ausführen von Ransomware und anderer Schadsoftware kann auf folgende Art erschwert werden:

- **Filterung am Web-Proxy**

  Bei Windows-Clients, die nicht direkt sondern nur über einen Proxy mit dem Internet kommunizieren dürfen, ist es eine effektive Maßnahme, den Download der eigentlichen Ransomware bereits am Proxy zu unterbinden.

Zusätzlich zur Filterung nach Dateitypen (.exe, .vbs, .scr, …) hat sich die URL-Reputation als hilfreiches Kriterium erwiesen.

Ransomware-Kampagnen arbeiten aktuell meist noch unter Zuhilfenahme von unverschlüsselten http: URLs zum Herunterladen des Executables. Es ist zu erwarten, dass die Angreifer in Zukunft auf https: wechseln. Es werden auch bekannte Webdienste wie Dropbox, GitHub, etc. missbraucht.

- **Application Whitelisting**

  Microsoft AppLocker (oder Software Restriction Policies) bzw. entsprechende Produkte anderer Hersteller können dazu benutzt werden, genau zu definieren, welche Programme auf einem Windows-PC ausgeführt werden dürfen.

  Ein restriktives Whitelisting der legitimen Programme ist oft mit einem erheblichen Verwaltungsaufwand verbunden. Wo dies nicht sinnvoll erscheint, kann mit diesen Werkzeugen zumindest die Programmausführung in bestimmten Verzeichnissen unterbunden werden. Im Kontext Ransomware sind das vor allem die Ordner/Unterordner: %LocalAppData%, %AppData% und %TEMP%. Auch diese Einstellungen sollten auf unerwünschte Seiteneffekte getestet werden.

Schadensbegrenzung

Folgende Maßnahmen können die Auswirkungen einer Ransomware Infektion begrenzen:

- **Backups**
  Aktuelle, sichere und verfügbare Sicherheitskopien Ihrer Daten sind ein wirkungsvolles Mittel gegen die Auswirkungen von Ransomware. Das mag trivial klingen, die Erfahrung hat jedoch gezeigt, dass insbesondere bei Kleinstunternehmen und Privatpersonen die Backupstrategie oft nicht ausreichend ist.

  Wichtig ist, dass die Backups nicht von der Ransomware mit verschlüsselt werden können. So ist etwa eine dauerhaft an den PC/Server angesteckte USB-Platte für solche Fälle kein wirksames Backup.

  Bei Backups in die „Cloud“ muss sichergestellt werden, dass auch auf „alte“ Versionen der gesicherten Dateien zugegriffen werden kann. Im schlimmsten Fall werden bei der Synchronisation mit der Cloud die Kopien dort durch die bereits von der Ransomware verschlüsselten Dateien überschrieben.

  Die empfohlene Frequenz von Backups hängt vom Umfeld ab, für Firmen ist ein tägliches Backup in den meisten Fällen sinnvoll. Regelmäßiges Testen und Üben der Wiederherstellung von Daten gehört genauso zu einer guten Backupstrategie wie längerfristiges Aufheben von einzelnen Backupständen.

- **Zugriffsrechte**

  Aktuelle Ransomware-Varianten arbeiten mit den Rechten des angemeldeten Benutzers. Je weniger Daten dieser Benutzer überschreiben kann, umso geringer ist der potentielle Schaden. Ein striktes Rechtemanagement auf Fileshares ist daher zu empfehlen.

- **Verhaltensbasierte Erkennung**

  Es gibt Lösungsansätze, die speziell auf Ransomware abgestimmt sind:

  - Malwarebytes stellt ein entsprechendes Tool[10] zu Verfügung. Diese ist aber noch als Beta eingestuft und noch nicht für den Produktivbetrieb geeignet.
  - Werden am Fileserver die Schreibzugriffe mitgeloggt, lassen sich übliche Werkzeuge zur Loganalyse darauf ansetzen. Der Heise-Verlag hat dies für Samba mittels fail2ban in einem Artikel[11] beschrieben.

Richtige Reaktion im Schadensfall

Ruhe bewahren.

- **Falls der Verschlüsselungsprozess noch läuft**

  Üblicherweise werden bei der Verschlüsselung die Dateien nacheinander abgearbeitet. Es bietet sich daher an, die Verbindung zum betreffenden Datenträger zu unterbrechen, um die noch nicht verschlüsselten Dateien zu „retten". Die folgende Aufstellung beschreibt die dabei möglichen Szenarien:

Betroffener Datenträger	Wo läuft die Ransomware?	Mögliche Aktionen
Fest eingebaut (HD oder SSD am internen SATA-Anschluss, …)	Lokal	• Stromzufuhr unterbrechen
Extern (USB-Stick, USB-Festplatte, …)	Lokal	• Datenträger abstecken • Stromzufuhr unterbrechen
Netzwerk-Share	Client	• Netzwerkkabel[12] vom Client ziehen • Stromzufuhr vom Client unterbrechen • Netzwerkkabel vom Share ziehen • Stromzufuhr vom Share unterbrechen

[10] https://forums.malwarebytes.org/topic/177751-introducing-malwarebytes-anti-ransomware/
[11] http://www.heise.de/security/artikel/Erpressungs-Trojaner-wie-Locky-aussperren-3120956.html
[12] Auch WLAN-Adapter (Fallbacks?) bedenken!

Cloud-Volume	Client	• Netzwerkkabel vom Client ziehen • Stromzufuhr vom Client unterbrechen

Diese Aktionen haben potentiell negative Seiteneffekte:

- Die gerade in Verschlüsselung befindlichen Dateien könnten in einen undefinierten Zustand kommen.
- Ein Kontakt zum Angreifer könnte unterbrochen werden und somit eine mögliche Entschlüsselung nach einer Zahlung des „Lösegeldes“ erschwert werden.

- **Verschlüsselte Datenträger aufbewahren**

  Wenn die von der Verschlüsselung betroffenen Datenträger nicht unmittelbar benötigt werden, empfiehlt es sich, diesen (und nicht nur die einzelnen Dateien) aufzuheben. Es besteht eine geringe Hoffnung, dass Werkzeuge verfügbar werden, die eine spätere Entschlüsselung möglich machen.

- **Wiederherstellung eines sicheren Betriebs**

  In vielen Fällen verschlüsselt Ransomware nur die Daten, ohne eine tiefergehende Infektion des betroffenen Systems. Das System stand aber unter fremdem Einfluss und ist daher als kompromittiert einzustufen.

- **Soll man auf die Geldforderung eingehen?**

  Hier gibt es moralische, rechtliche und wirtschaftliche Aspekte. Wir raten, keine voreiligen Entscheidungen zu treffen, sondern nüchtern abzuwägen[13].

  Eine Garantie, dass man nach der Bezahlung auch wirklich Zugriff auf seine Daten wiedererlangt, gibt es nicht. Andererseits wissen die Angreifer genau, dass ihr Geschäftsmodell davon abhängt, dass bekannt ist, dass die Entschlüsselung funktioniert[14]. Die Erfolgswahrscheinlichkeit des Zahlens ist daher nicht schlecht.

- **Wiederholungen vermeiden**

  Nachdem der Vorfall bearbeitet wurde, sollte jedenfalls versucht werden, aus den Geschehnissen für die Zukunft zu lernen.

[13] https://nakedsecurity.sophos.com/2015/10/28/did-the-fbi-really-say-pay-up-for-ransomware-heres-what-to-do/
[14] http://www.nytimes.com/2015/01/04/opinion/sunday/how-my-mom-got-hacked.html

Quellen

- Wikipedia (DE / EN)
- BSI: Ransomware: Bedrohungslage, Prävention & Reaktion
- Tipps von Robert Penz
- SANS ISC Blog
- Tripwire: 22 Ransomware Prevention Tips
- Christiaan Beek: "There's a pot of Bitcoins behind the ransomware rainbow"
- Futurezone / Michael Krausz
- IKARUS Blogeintrag
- Tim Anderson
- Heise Security: Fail2ban, Malwarebytes tool
- ACSC: Hardening MS Office 2013
- Ars Technica: Ransomware via Ad-Networks
- Microsoft MMPC: Samas Ransomware
- Talos: Die Kryptographie hinter TeslaCrypt 3
- Sophos: Über die Empfehlung des FBI
- ThirdTier: CryptoLocker Warning