VII. Ransomware (Online-Erpressungen)

1. Phänomenbeschreibung

Ransomware ist der Kategorie **Scareware** zuzuordnen, also der Schadsoftware, die den Nutzer erschrecken bzw. ihm Angst einjagen soll, um ihn am PC Handlungen ausführen zu lassen, die er sonst nicht tätigen würde. Der Name setzt sich aus dem englischen Wort *ransom* für Erpressung und *ware* für Schadsoftware (nicht nur Ware) zusammen.

Klassische Scareware suggeriert dem Betroffenen, dass dessen **Computer mit Viren befallen** ist. Die Täter bereichern sich dabei auf verschiedenen Wegen: Es wird eine günstige Software zum Download angeboten, die von der angeblichen Malware befreien soll. Dabei handelt es sich jedoch um eine meist nutzlose Anwendung, die keinerlei Schutz bietet. Eine andere Variante besteht darin, dass ein zunächst kostenloser Download eines Programmes angeboten wird, welches scheinbar das Problem behebt. Nach wenigen Tagen schlägt der kostenlose Virenscanner erneut an und berichtet, dass ein so schweres Sicherheitsrisiko vorliegen würde, welches mit der kostenlosen Version nicht mehr behoben werden könne. Es wird zum Kauf eines teuren Produktes aufgefordert.

Es gibt auch vermeintliche Antivirenschutz-Programme, die nach der Installation persönliche Daten verschlüsseln. Erst nach der Zahlung eines „Lösegeldes" werden diese wieder entschlüsselt. Aufgrund dieses Nötigungsmittels liegt dann bereits eine **Ransomware** vor.

Ransomware wie zum Beispiel „Ukash- oder BKA-Trojaner" bzw. „.zip-Trojaner" sperrt hingegen den infizierten Rechner, sodass an diesem kein Arbeiten mehr möglich ist. Nur gegen eine vorgebliche „Strafzahlung" via elektronischem Zahlungsmittel soll dieser wieder frei geschaltet werden.

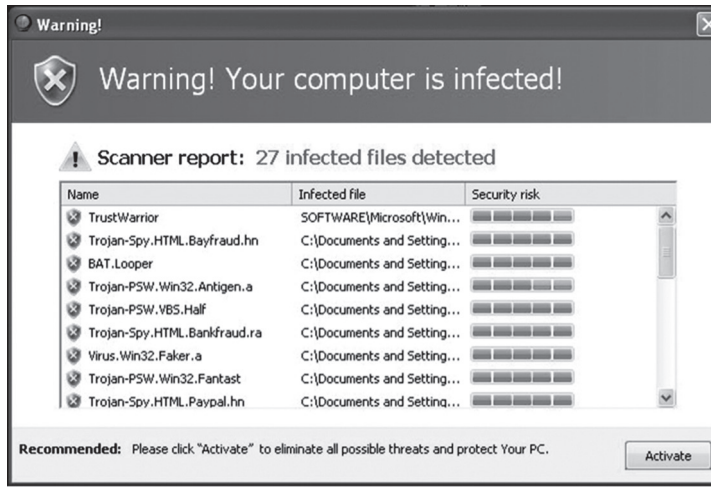

Abbildung 11: Diese Scareware meldet zahlreiche Viren, die angeblich auf dem Rechner festgestellt worden sind.

2. Die Infizierung erfolgt derzeit über zwei verschiedene Wege

2.1 Drive-by-Download

Über den so genannten **Drive-by-Download**, also dem unbewussten und unbeabsichtigten Herunterladen der Software während des Besuches des Nutzers auf einer inkriminierten Website. Auf dem Rechner selbst installiert sich die Malware dann ebenfalls unbemerkt und manipuliert den Autostart des betroffenen Systems. Ziel ist es dabei, bei jedem Neustart auch den Trojaner neu zu starten. Daneben wird durch dieses Vorgehen auch die Entfernung der Schadsoftware erschwert.

Zur Platzierung der Malware auf regulären Seiten des Internets werden von den Tätern Schwachstellen des Systems ausgenutzt und das Schadprogramm in einem Link oder einem Download dieser Seite hinterlegt. Klickt der Nutzer unbedarft darauf, wird die Installation ausgelöst. Bei manchen Varianten werden neben der Installa-

tion der Ransomware zeitgleich Dateien (überwiegend Office Anwendungen) auf dem infizierten Rechner verschlüsselt. Damit soll der Geschädigte mit Nachdruck aufgefordert werden, sofort einen geldwerten Voucher von Paysafe oder Ukash zu erwerben. Wurden zu Beginn der Schadenswelle überwiegend Seiten mit erotischen Inhalten manipuliert, erfolgt die Verbreitung neben „alltäglichen Websites“ (auch renommierte Seiten wurden bereits erfolgreich angegriffen, sodass der Rechner eines Nutzers durch bloßes Lesen von Nachrichten infiziert wurde) mittlerweile auch über soziale Netzwerke. Dort wird sie in einem Anhang des Absenders integriert. Dieser Anhang soll von einem vermeintlichen Freund im gemeinsamen sozialen Netzwerk stammen und wird deshalb unter Umständen keiner oder nur eine oberflächlichen Prüfung unterzogen. Der Erfolg der Täter ist in diesem Fall ungemein höher.

2.2 .zip-Trojaner

Eine weitere Methode ist der **Versand von manipulierten E-Mails**. Diese Variante ist unter dem Begriff **.zip-Trojaner** bekannt. Der Geschädigte erhält beispielsweise eine E-Mail mit einer Bestellbestätigung augenscheinlich von Amazon. Einzelheiten und Stornierungsmöglichkeiten seien im Anhang zu finden. Bei diesem Anhang handelt es sich meist um eine .zip-Datei, selten auch um eine .pdf-Datei. In beiden Fällen installiert sich nach dem Anklicken die Ransomware und legt den Rechner lahm.

Die Täter sind dabei recht kreativ. Es werden E-Mails vom Finanzamt gefälscht, mit der Ankündigung einer Steuernachzahlung. Ein beiliegendes Formular sei deswegen auszufüllen. Auch gefälschte Monatsrechnungen von diversen Handyprovidern werden versandt. Durch hohe Gebühren wird der Empfänger dazu verleitet, den angegebenen Link aufzurufen, um sich näher über die unüblich hohen Kosten zu informieren.

Surft der Nutzer auf einer inkriminierten Webseite oder ruft er den manipulierten Anhang einer Nachricht ab, öffnet sich für ihn irgendwann und nicht vorhersehbar ein Popup-Fenster. Das Design dieses Fenster suggeriert dem Nutzer, dass die Nachricht beispielsweise vom Bundeskriminalamt stammt: Farbgebung, Aufmachung sowie

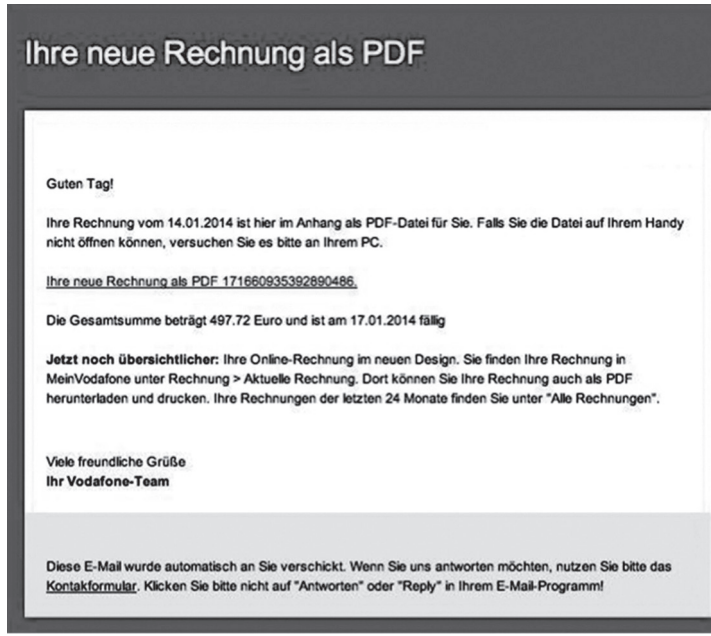

Abbildung 12 zeigt eine vorgebliche Rechnung der Fa. „Vodafone“. Hinter dem Link, der angeblich zur PDF der Rechnung führt, verbirgt sich jedoch ein Schadcode, der nach Anklicken eine Malware auf dem Rechner installiert.

Stern und Name der Polizeibehörde vermitteln eine offizielle Nachricht. Darin wird dem Nutzer mitgeteilt, dass sein Rechner vom BKA gesperrt wurde. Grund hierfür sei, dass er in Zusammenhang mit Kinderpornographie, sodomistischen Handlungen und Gewalt in Erscheinung getreten sei. Zudem seien vom betroffenen Computer Mails mit terroristischen Inhalten versandt worden. Um zu vermitteln, dass dies sich auch so zugetragen hat, werden in der Meldung die IP-Adresse des betreffenden Computers, dessen Betriebssystem sowie der verwendete Browser angezeigt. Inzwischen firmiert die Schadsoftware auch unter dem Label der Verwertungsgesellschaft GEMA, da angeblich nicht lizensierte Musikstücke aus dem Netz geladen worden seien, oder der Gebühreneinzugszentrale GEZ. Hier wird behauptet, dass der Nutzer Musikstücke anhört und

Videofilme ansieht, ohne die dafür erforderliche Rundfunkgebühr entrichtet zu haben. Ziel ist es in allen Fällen, Geld vom PC-Nutzer zu erhalten.

Abbildung 13 zeigt eine Variante des sog. „BKA-Trojaners“.

Zwischenzeitlich gibt es mehrere Dutzend verschiedener Bildschirmdarstellungen. Ein Überblick ist auf der Webseite www.bka-trojaner.de zu finden. Hier werden zudem Möglichkeiten beschrieben, wie die Ransomware wieder beseitigt werden kann.

In den Anfängen der Verbreitung der Erpressersoftware sollten die betroffenen Nutzer angegebene Telefonnummern anrufen um auf diesem Wege zu erfahren, wie ihr Computer wieder freigeschaltet werden könne. Dabei fielen hohe Gebühren an, die dem Täter zukamen. Eine Variation dieser Methode war die Verschlüsselung von Daten auf fremden Rechnern, die dem Eigentümer dann als beschädigt angezeigt wurden. Um seine Datensätze wieder reparieren zu können, wurde dem Geschädigten angeboten, die Freeware einer Reparatursoftware zu laden (beispielsweise „Data Doctor 2010“). Nach der Aktivierung der heruntergeladenen Software blieben allerdings noch einige Daten verschlüsselt bzw. „beschädigt“. Diese

könnten angeblich nur gerettet werden, wenn die kostenpflichtige Vollversion der Reparatursoftware gekauft und angewandt würde.

In der aktuellen Variante verlangt der Täter die Bezahlung einer „Strafe“ innerhalb von 24 Stunden. Damit er über Kontobewegungen nicht zurückverfolgt werden kann, nutzt der Täter das **Bezahlsystem Ukash**. Zur Abwicklung des Geschäfts, an dessen Ende die Freischaltung des PC stehen würde, soll der geschädigte Nutzer einen Ukash-Voucher erwerben. Den darauf angegebenen 19-stelligen Code soll er in das auf der Sperrseite eingerichtete Textfeld eingeben. Zur Untermauerung der Forderung werden entweder in einem festen Rhythmus Dateien gelöscht oder aber angedroht, die gesamte Festplatte zu löschen. In den meisten Fällen wird die Blockade jedoch nicht aufgehoben – auch wenn bezahlt wurde. Im Gegenteil: Es werden manchmal auch Nachforderungen erhoben. Die Methode, mit einer nachgemachten Seite, die vortäuscht eine offizielle Polizeiseite zu sein, Geld zu machen, ist nicht allein auf Deutschland beschränkt. In Großbritannien kommt beispielsweise die „Metropolitan-Police-Ransomware“ zum Einsatz. Das Prinzip ist dasselbe wie hierzulande.

3. Strafrechtliche Relevanz

Versand von manipulierten E-Mails:

§ 263 a StGB i.V.m. § 263 Abs. 2 StGB (Versuchter Computerbetrug) kommt in Betracht, wenn der Täter eine Mail mit der Absicht versendet, den Computer des Empfängers zu sperren und damit Geld zu fordern.

§ 269 StGB (Fälschung beweiserheblicher Daten) ist zu prüfen, wenn ein Name einer tatsächlich existierenden Firma oder Organisation missbraucht wird und dadurch der Eindruck entsteht, die Aufforderung beispielsweise einen Anhang zu öffnen, hat einen amtlichen bzw. reellen Hintergrund.

§ 303a StGB (Datenveränderung) in der Variante der Unbrauchbarmachung oder Veränderung von Daten, wenn der Empfänger den Mailanhang öffnet und der Computer infiziert wird. Sollte die Datenverarbeitung für den Nutzer von wesentlicher Bedeutung sein und die Daten konnten nicht wieder ohne großen eigenen Aufwand

hergestellt werden, ist **§ 303b StGB** (Computersabotage) zusätzlich zu prüfen.

Nachdem der Geschädigte den Anhang (.zip-Datei) geöffnet hat, gibt es zwei Varianten: Er erkennt, dass er einem Fake aufgesessen ist und bezahlt nicht, kann ein versuchter Computerbetrug nach **§ 263a StGB i.V.m. § 263 Abs. 2 StGB** vorliegen. Bezahlt er dagegen in Glauben, die Forderung begleichen zu müssen, ist der Computerbetrug mit dem Eintritt der Schädigung vollendet: **§ 263a StGB**.

Die Ransomware installiert sich nach Öffnen einer inkriminierten Seite:

§ 303a Abs. 1 StGB (Datenveränderung mit der Variante der Datenunterdrückung), da der PC gesperrt wird und nicht mehr nutzbar ist. Der Tatbestand ist erfüllt, wenn die Daten auch nur vorübergehend unterdrückt und sie nach der Entfernung des Virus wieder nutzbar sind. Nach **§ 303a Abs. 2 StGB** ist der Versuch strafbar.

303b StGB (Computersabotage), falls die Datenverarbeitung für den Nutzer von wesentlicher Bedeutung ist und die Daten nicht wieder ohne großen eigenen Aufwand hergestellt werden konnten. Nach **§ 303b Abs. 3 StGB** ist der Versuch ebenfalls strafbar. Sollte bei einer individuellen Tatbeurteilung der Tatbestand nach § 303b Abs. 1 Nr. 1 StGB festgestellt werden, so tritt im Rahmen der Konkurrenz § 303a Abs. 1 StGB zurück.

§ 202c Abs. 1, Nr. 2 StGB (Vorbereiten des Ausspähens und Abfangens von Daten), wenn die Schadsoftware programmiert, sich oder einem anderen verschafft, verkauft, einem anderen überlassen, verbreitet oder sonst zugänglich gemacht wird, **um** eine Tat nach §§ 303a, 303b StGB zu begehen. Nach **§ 303c StGB** ist ein Strafantrag notwendig, wenn die Voraussetzungen des § 303b Abs. 1 bis 3 StGB erfüllt sind.

§ 253 StGB (Erpressung), wenn dem Anwender mit einem empfindlichen Übel, wie z. B. dem Löschen der Daten auf seinem Rechner, gedroht wird und er aufgrund dieser Drohung genötigt wird, Geld zu bezahlen damit dies vermeintlich nicht geschieht. Als Folge muss dem Opfer ein Vermögensnachteil entstehen und sich der Täter in dessen Folge zu Unrecht bereichern.

4. Zivilrechtliche Relevanz

§ 823 Abs. 1 BGB (Schadenersatzpflicht – allgemeine Haftungsgrundlagen) wie zum Beispiel einer Nutzungsbeeinträchtigung durch einen für eine gewisse Dauer gesperrten Computer oder dem Verlust von Geld und ggf. **§ 823 Abs. 2 BGB** (Schadenersatzpflicht – Verletzung von Schutzgesetzen), wenn nach einer Prüfung festgestellt wird, dass es sich bei den §§ 253, 303a und 303b StGB um solche zur Erfüllung des Tatbestandes notwendige Schutzgesetze handelt und eine vorsätzliche Begehung vorliegt.

5. Checkliste für die Ermittlungspraxis

Die Sperrbildschirme weisen in der Regel die gleichen Inhalte auf. Deshalb ist vorab dieser Inhalt zu prüfen und festzustellen, ob er einer bereits bestehenden Welle zugeordnet werden kann. Augenmerk ist dabei auf die absendende Institution (z. B. Polizei, BKA, Bundespolizei, GEMA, GUV, BSI), die Höhe sowie die Art und Weise der Zahlungsaufforderung, deren Abwicklung und deren Folgen, die Drohung der Konsequenzen bei Nichtbezahlung, die Anzeige der Nutzerdaten des infizierten PC (IP-Adresse, Provider, Betriebssystem, Browser, Standort des PC) zu legen. Kann bei der Prüfung festgestellt werden, dass es sich um eine bereits bekannte Welle handelt, ist die Abgabe des Vorgangs zu einem Sammelverfahren zu prüfen. Handelt es sich um neu programmierte Malware, wird die Strafanzeige an die für den Tatort zuständige Staatsanwaltschaft abgegeben.

Folgende Maßnahmen sind durchzuführen:

- ✓ Der **erste Angriff** erfolgt durch die Schutzpolizei, die Endsachbearbeitung durch die Kriminalpolizei.
- ✓ Zeugenbefragung, welche Variante vorliegt: Wurde E-Mail mit Anhang geöffnet oder geschah der Vorfall nach bloßem Surfen.
- ✓ Je nach Antwort:
- ✓ Festhalten der zuletzt betrachteten Webseiten.
- ✓ Sicherstellung der E-Mail incl. Anhang: E-Mail-Header auslesen.
- ✓ Anhang (.zip-Datei) speichern (USB, CD) oder nach Rücksprache an Fachdienststelle.

- ✓ Weiterleitung der E-Mail an ein spezielles E-Mail-Postfach (ohne Filterung).
- ✓ Erfolgte der Kauf eines Vouchers? Falls ja: Code und Kaufpreis erheben, Kopie des Voucher fertigen.
- ✓ Geschädigten darauf hinweisen, dass er den Code sperren lassen und sich das Geld erstatten lassen kann. Entsprechende Hinweise und Formblätter sind online beim jeweiligen Finanzdienstleister zu finden.
- ✓ Zeitnahe Abgabe an die Fachdienststelle zur Auswertung etwaig verwendeter Voucher.
- ✓ Rücksprache mit der Fachdienststelle bzw. Beachtung der örtlichen Besonderheiten, ob PC des Geschädigten generell oder im Einzelfall forensisch untersucht werden soll.

6. Präventionsmaßnahmen

Grundsätzlich gilt, dass eine aktuelle Virenschutzsoftware installiert ist. Diese sollte, ebenso wie das Betriebssystem des Rechners, durch Updates aktuell gehalten werden. Mit der Virenschutzsoftware sollte nicht nur die aktuelle Sitzung am PC überwacht, sondern Festplatte und Speichermedien regelmäßig gescannt werden. Ferner sollten eigene und vor allem fremde Speichermedien (USB-Sticks, DVD/CD, externe Festplatte) vor dem Öffnen auf Viren geprüft werden.

Auf dem PC sollte eine Firewall installiert sein.

Java sollte deaktiviert sein und nur bei wirklichem Bedarf kurzzeitig und manuell aktiviert werden.

Für jede Anwendung sollte ein eigenes Passwort generiert worden sein, dass regelmäßig geändert wird. Das Passwort nicht auf dem PC speichern bzw. neben dem PC verwahren.

Für Benutzer des PC sollten eigene Benutzerkonten ohne Administratorenrechte eingerichtet werden. Der Administrator erhält ein eigenes Konto. Alle Konten sollten jeweils mit einem Passwort versehen werden.

Darüber hinaus sollte beim Surfen im Netz genau gelesen werden, ob nach dem Seitenaufruf auch in der Adresszeile die Mailadresse steht, die besucht werden sollte.

Die in Webseiten (auch in seriösen) eingebundenen Links nicht wahllos anklicken.

Regelmäßig sollten die sich auf dem Rechner befindlichen Daten gespeichert werden.

Erkennen von manipulierten Links

Allein die Gestaltung und Formulierung einer E-Mail lässt keinen Schluss mehr zu, ob es sich um eine Original-E-Mail oder um eine Fälschung handelt. Ferner können in diesen E-Mails auch alle Links frei benannt werden und müssen nichts mit der Originalseite zu tun haben. Welche Links nach dem Anklicken tatsächlich aufgerufen werden, lässt sich überprüfen, indem man mit dem Mauszeiger ohne zu klicken auf dem jeweiligen Link verweilt. Hier wird dann die tatsächliche Linkadresse angezeigt. Wie auf dem folgenden Bild einer falschen Bestellbestätigung zu erkennen ist, wird eine Webseite in Ungarn aufgerufen. Diese Webseite mit der Domain „www.adnatura.hr“ wurde offensichtlich gehackt. Anschließend wurde die im Design von Amazon nachgebildete inkriminierte Seite von der Täterschaft auf dem Server in einem eigens eingerichteten Unterordner gehostet. Wird der Link angeklickt, erfolgt der Drive-by-Download einer Malware.

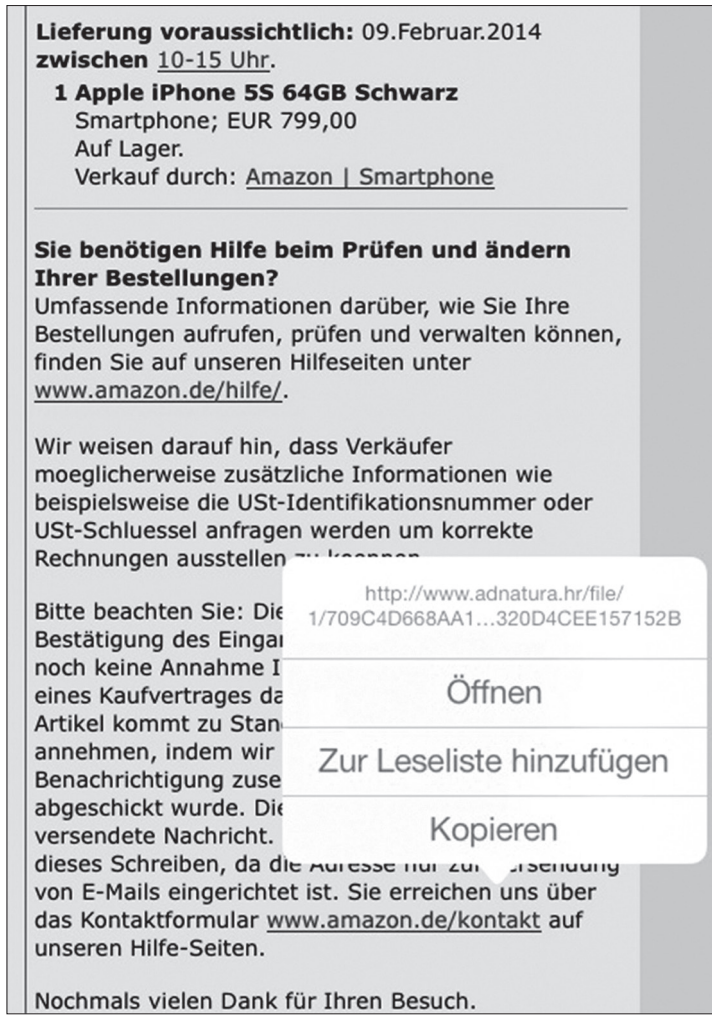

Abbildung 14 zeigt eine angebliche Mail von „Amazon“. Alle dort aufgeführten Links führen nicht zu Amazon, sondern zu einer manipulierten Webseite (http://www.adnatura.hr/file/...), wo nach dem Aufruf gefährliche Malware heruntergeladen wird.