Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Ransomware

Bedrohungslage 2022

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

Inhalt

1 Einleitung

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.

Die Bedrohungslage durch Ransomware ist hoch. Es treten inzwischen häufig Fälle auf, über welche öffentlich berichtet wird und bei denen zuvor gestohlene Daten veröffentlicht werden. Weil der Leidensdruck für die Betroffenen hoch ist, zahlen Opfer in vielen Fällen das geforderte Lösegeld.

Bereits seit 2010 / 2011 wird Ransomware verbreitet für Cyber-Angriffe eingesetzt. Auch davor gab es 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 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.

2 Bedrohungslage

Ransomware ist 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. Die Bedrohungslage durch Ransomware ist für Institutionen hoch.

Ransomware-Vorfälle zeichnen sich durch folgende Punkte aus.

- Hoher Leidensdruck beim Opfer durch direkte Auswirkungen im Betrieb
- Es ist teilweise billiger für die Geschädigten auf die Erpressung einzugehen, als wenn länger Verluste durch Produktionsstillstand oder Wiederherstellung erlitten werden müssen.
- Zahlung in Bitcoins oder Monero sind anonym und sofort realisierbar. Sie müssen von den Angreifenden nicht aufwändig über Geldboten/Moneymules und Warenagenten gewaschen werden.

2.1 Angriffsvektoren

Die wichtigsten Infektionsvektoren von Ransomware sind hierbei insbesondere Spam-Mails mit schadhaften Anhängen oder verlinkter Schadsoftware, sowie Schwachstellen in aus dem Internet erreichbaren Server-Systemen.

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 passwortgeschützte 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.

Verschiedene Schadsoftware-Varianten haben das Spammen optimiert. Diese können auf infizierten Systemen Kontakte und legitimen E-Mails ausspähen. Anschließend werden Spam-Mails als vermeintliche Antworten auf entsprechende tatsächliche E-Mails versendet. Die bekannten Betreffzeilen und Zitate einer vorhergehenden Kommunikation lassen die Spam-Mails für die Empfänger noch authentischer erschienen.

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 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 Mehr-Faktor-Authentifizierung.

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 und infizierten das jeweilige System.

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

2.2 Potentielle Schäden

Schäden für eine Organisation durch Cyber-Sicherheitsvorfälle kann man in

- Eigenschäden,
- Fremdschäden und
- Reputationsschäden

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 Veröffentlichung von Daten).

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 abgewendet werden konnte, kann eine gute Bewältigungsstrategie den Schaden erheblich begrenzen. Das Schadensausmaß reicht dabei von "Lässt sich innerhalb kurzer Zeit identifizieren und abschalten" über "Nach 4 Stunden sind die betroffenen Datenbestände wiederhergestellt und es kann normal weitergehen" bis hin zu "Wochenlang kann nur eine Notfallversorgung angeboten werden".

Dabei können u. a. folgende entscheidende Einflussfaktoren für das Schadensausmaß sein:

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 verfügbar 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.

2.3 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]
Mindestens eine Gruppe veröffentlicht Daten sogar in einem für Dritte durchsuchbaren Format[2].

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

2.4 Motivation des Täters

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 Sicherungssysteme. 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:

[1] https://www.golem.de/news/finnland-datenleck-von-psychotherapie-klinik-fuer-erpressung-genutzt-2010-151742.html
[2] https://blog.cyble.com/2022/07/06/alphv-ransomware-expands-its-arsenal-of-extortion-techniques/

- 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. Firmen laufen beim Verlust des Zugriffs auf Daten Gefahr, insolvent zu werden.

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.

Die finanzielle Motivation kann auch von staatlichen Angreifenden kommen. Diese versuchen für Ihren Staat beispielsweise Sanktionen zu umgehen und Devisen zu beschaffen.

Eine weitere Motivation zur Verbreitung von Ransomware kann die Sabotage sein. Hierfür wird statt Ransomware ein sogenannter Wiper verwendet. Die Sabotage 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, ein Wiper der 2017 in der Ukraine und international großen Schaden anrichtete, ging bei den Betroffenen keine Erpressungsmeldung ein und den Nutzern wurde keine Möglichkeit gegeben, die 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.
Ransomware kann auch genutzt werden, um von vorhergehenden Spionage-Operationen abzulenken und stattdessen die Indizien auf kriminelle Angreifenden deuten zu lassen.

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“
- Erreichen von Zielen von Hacktivisten

2.5 Organisation der Angreifenden

Basierend auf im Februar 2022 geleakten Informationen zur Gruppe „Conti“ zeichnet sich ein Bild von Angreifenden, die sich wie ein „normales“ Start-Up organisiert haben.

Die Arbeitsweise ist arbeitsteilig organisiert. Es gibt einen Chef, Systemadministratoren, Entwickler, die eigentlichen „Hacker“, Lösegeld-Verhandler und Personaler[3]. Die einzelnen Teams haben jeweils eigene Leiter. Der initiale Zugang zu einem Opfer-Netzwerk wird häufig von anderen Gruppen eingekauft, die sich auf die Zugangsbeschaffung spezialisiert haben, hierzu gibt es entsprechende Verbindungspersonen. Diese Gruppen sind auch als Access Broker bekannt. (Siehe auch Kapitel Phase V: Criminal Service für alles)

Die Art der Bezahlung innerhalb der „Conti“-Gruppe ist abhängig von der Stellung. Während Personen im Personalmanagement vermutlich ein fixes Gehalt erhalten, erhalten die Verhandler einer Lösegeldsumme einen prozentualen Anteil hiervon. Daneben kann es bei kritischen Fehlern oder unzureichenden Leistungen Abzüge vom Gehalt geben, während herausragende Leistungen mit Zuschlägen entlohnt werden.

Insgesamt lässt sich bei Ransomware-Gruppen sowie auch bei anderen cyberkriminellen Akteuren eine organisatorische Professionalisierung beobachten. Ein weiteres evidentes Beispiel hierfür ist die Entwicklung von Cybercrime als Service. (Siehe auch Kapitel Phase V: Criminal Service für alles)

[3] Eine detaillierte Beschreibung der Bereiche kann beispielsweise unter https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/ nachgelesen werden.

3 Lage in den Unternehmen

Bei Ransomware-Vorfällen treten Versäumnisse bei der Prävention 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 (siehe dazu den 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 in 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.

Besondere Vorfälle

Für diese Fallsammlung wurden ausschließlich Informationen öffentlicher Quellen genutzt!

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: [4],[5],[6],[7]

Colonial Pipeline

Am 7. Mai 2021 wurde in den USA der Pipeline-Betreiber Colonial Pipeline von der Ransomware DarkSide angegriffen und verschlüsselt. Infolge dessen stellte das Unternehmen den Betrieb mehrere Tage ein, es kam in zahlreichen Bundesstaaten zu Engpässen bei Kraftstoffen und Panikkäufen, ein regionaler Notstand wurde ausgerufen.

Das Unternehmen zahlte Lösegeld von mehreren Millionen Dollar, die Wiederherstellung über das von den Angreifern bereitgestellte Tool dauerte aber so lange, dass das Unternehmen dennoch weiterhin auf vorhandene Backups zurückgreifen musste.

Quellen: [8], [9], [10], [11], [12]

Costa Rica

Mitte April 2022 wurden Dutzende Institutionen des Landes Costa Rica von der Gruppe Conti angegriffen und zahlreiche Daten veröffentlicht. Der Vorfall hatte insbesondere Auswirkungen auf den Außenhandel, Lohnzahlungen und Ermittlungen der Staatseinnahmen und -ausgaben. Die Regierung rief den nationalen Notstand aus. Der Präsident der Republik erklärte das sogar als „Krieg“ gegen internationale „Cyber-Terroristen“.

Quellen: [13], [14], [15], [16]

[4] https://www.spiegel.de/netzwelt/netzpolitik/norsk-hydro-hackerangriff-war-eine-lockergoga-ransomware-attacke-a-1258627.html
[5] https://www.kaspersky.de/blog/hydro-attacked-by-ransomware/18804/
[6] https://www.hydro.com/nl-nl/media/news/2019/update-on-cyber-attack-march-26/
[7] https://www.inside-it.ch/articles/53971
[8] https://www.tagesschau.de/ausland/amerika/benzinengpaesse-usa-hackerangriff-101.html
[99] https://www.tagesschau.de/ausland/usa-pipeline-hackerangriff-101.html
[10] https://www.tagesschau.de/ausland/usa-notstand-pipeline-101.html
[11] https://www.tagesschau.de/wirtschaft/unternehmen/colonial-pipeline-loesegeld-hacker-angriff-ransomware-101.html
[12] https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom
[13] https://www.nacion.com/el-pais/servicios/hacienda-micitt-imn-y-racsa-atacados-por-hackers/DMCT7BZYIZGHZIHQQPOKN2WWYM/story/
[14] https://www.netzwoche.ch/news/2022-05-11/costa-rica-erklaert-nach-ransomware-attacke-nationalen-notstand
[15] https://www.heise.de/news/Ransomware-Befall-Notstand-in-Costa-Rica-Erpressergruppe-veroeffentlicht-Daten-7079285.html
[16] https://delfino.cr/2022/05/chaves-afirma-que-pais-esta-en-guerra-por-ataques-ciberneticos-y-que-habria-ticos-ayudando-a-conti

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: [17],[18],[19],[20]

Funke Medien Gruppe

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.

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: [21],[22],[23],[24],[25]

[17] https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/krankenhaus-derzeit-nur-sehr-eingeschraenkt-erreichbar-patientenversorgung-eingeschraenkt
[18] https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/uniklinik-duesseldorf-wieder-bereit-fuer-notfaelle
[19] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/UKDuesseldorf_170920.html
[20] https://www1.wdr.de/nachrichten/rheinland/uniklinik-duesseldorf-erpressung-hacker-100.html
[21] https://www.heise.de/news/Trojaner-Angriff-Ransomware-legt-Funke-Mediengruppe-lahm-4998302.html
[22] https://www.heise.de/news/Funke-Tageszeitungen-erscheinen-trotz-Hackerangriffs-wieder-in-groesseren-Umfaengen-5000289.html
[23] https://www1.wdr.de/nachrichten/ruhrgebiet/hackerangriff-funke-mediengruppe-100.html
[24] https://www.faz.net/aktuell/feuilleton/medien/cyberangriff-funke-mediengruppe-von-hackern-attackiert-17115147.html
[25] https://hilfe.onleihe.de/pages/viewpage.action?pageId=16941113

4 Entwicklung von Ransomware

4.1 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 20.000 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[26].

4.2 Phase IIa: Effiziente Verbreitung und Zerstörung

Auch wenn es in den Jahren zuvor bereits technische Weiterentwicklungen gab, stellen die Jahre 2016 und 2017 eine 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[27] 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[28].

4.3 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[29]. 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.

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

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

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 wesentlicher Bestandteil der im Dokument „Maßnahmenkatalog Ransomware“ beschriebenen Maßnahmen.

4.4 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[30] 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 oder weitere Malware wie Trickbot abgedeckt. So erhalten die Angreifer in großem Umfang Informationen über ein Opfer, wie Betriebsgeheimnisse oder Umsatzdaten, und können Lösegeldforderungen entsprechend maßschneidern[31].

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.

4.5 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.

[30] 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.

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

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.[32]

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.

4.6 Phase V: Criminal Service für alles

Bereits seit Beginn der Professionalisierung cyberkrimineller Angriffe beobachtet das BSI einen Trend in Richtung cyberkrimineller Services, CCaaS. Zu diesen Services zählen u.a. Ransomware-as-a-Service (RaaS) als prominente Beispiele. Für einen cyberkriminellen Angreifer, der über die notwendigen Mittel und Verbindungen verfügt, kann zunehmend jeder Schritt eines Cyber-Angriffs aus Services zusammengestellt werden.

Für die Auslieferung von Malware gibt es Tools, die beispielsweise maliziöse Dokumente bauen. In Kombination mit einem Packing-Service, kann die darüber ausgelieferte Malware in einer Form gepackt werden, die eine Detektion bei der Auslieferung nach Möglichkeit verhindert. Diese Einzelschritte können aber auch direkt an einen Access Broker, im Sinne des Access-as-a-Service (AaaS), abgegeben werden. Von diesem kann sich ein Angreifer den Zugang zu einem Account oder auch einem ganzen Organisationsnetzwerk kaufen.

Die für einen Angriff notwendige Infrastruktur kann über einen Bullet-Proof Hoster beschafft werden. Dieser betreibt Internetinfrastruktur auf eine Art und Weise, die sie dem Zugriff der

[32] 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

Strafverfolgungsbehörden entzieht. Einige als Malware-as-a-Service (MaaS) angebotene Malware liefern eine eigene Infrastruktur auch gleich mit, welche beispielsweise aus kompromittierten Webauftritten besteht.

Für die Monetarisierung eines Cyber-Angriffs bieten sich cyberkriminellen Angreifern entsprechende Untergrundforen und Marktplätze an, auf denen beispielsweise gestohlene Daten verkauft werden können. Im Falle von RaaS wird Affiliates mitunter auch Unterstützung bei der Erpressung und Verhandlung mit den Opfern angeboten. Um das so eingenommene Geld durch Geldwäsche nutzbar zu machen, bieten sich wieder Untergrundmarktplätze und sogenannte Mixing-Dienste für Kryptowährungen an. Auf den Marktplätzen oder auch für wieder neue Dienstleistungen kann der Angreifer sein Geld direkt ausgeben.

Diese Service-Orientierung trägt dazu bei, dass mehr und mehr cyberkriminellen Angreifern professionelle und technisch-fortgeschrittene Methoden zur Verfügung stehen. Angreifer müssen diese Methoden nicht mehr selbstständig entwickeln oder sich aneignen. Es genügt, wenn ein marktführender Service eine Methode einführt, damit sie von einer Vielzahl an Angreifer direkt genutzt werden kann. Die Proliferation von Methoden unter den Service-Anbieter verstärkt diesen Effekt.

5 Weitere Informationen

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

5.1 Weitere Dokumente

- Maßnahmenkatalog Ransomware
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Massnahmenkatalog.html
- Managementabstrakt Fortschrittliche Angriffe
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Managementabstract-Angriffe.html
- Erste Hilfe bei einem schweren IT-Sicherheitsvorfall
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.html

5.2 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

5.3 Verteiler des BSI

Der Bundesverwaltung, VerwaltungsCERTs,Teilnehmern des UP KRITIS sowie der Allianz für Cyber-Sicherheit 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 Vorfallsinformationen
- BSI Themenlagebilder

Hinweis: Jedes Unternehmen bzw. jede Institution in Deutschland kann über eine kostenlose Mitgliedschaft in der Allianz für Cyber-Sicherheit[33] Zugriff auf die genannten Dokumente erhalten.

[33] https://www.allianz-fuer-cybersicherheit.de/