proofpoint.

Kurzinformation zu einer Bedrohung: **Ransomware**

Die Fakten

Beschreibung:

Ransomware verschlüsselt kritische Daten oder sperrt den Zugriff der Anwender auf ihre Geräte, bis ein meist hohes Lösegeld gezahlt wird. Die Angreifer stammen häufig aus dem Bereich der organisierten Kriminalität.

Ransomware-Tools:

Cryptolocker, WannaCry, Bad Rabbit, Cerber, Crysis, CryptoWall, GoldenEye, Jigsaw, Locky, Petya, Conti, Sodinokibi und Ryuk

Ursprung:

1989, Trojaner AIDS, der von Joseph Popp erstellt wurde. Popp sendete 20.000 infizierte Disketten mit der Aufschrift „AIDS Information – Introductory Diskettes“ an Teilnehmer der internationalen AIDS-Konferenz der WHO. Damit startete er die vermutlich weltweit erste Ransomware-Attacke.

Typen:

- **Krypto-Ransomware**
  Cyberkriminelle verschlüsseln die Dateien auf dem Computer, sodass der Anwender nicht mehr darauf zugreifen kann.
- **Locker-Ransomware**
  Diese Malware sperrt den Zugriff des Opfers auf den Computer, bis ein Lösegeld gezahlt wurde.
- **„Scareware“**
  Die Opfer sollen glauben, dass ihr Gerät mit Ransomware infiziert wurde, und Lösegeld bezahlen. Das ist zwar technisch gesehen keine Ransomware, hat aber den gleichen Effekt.

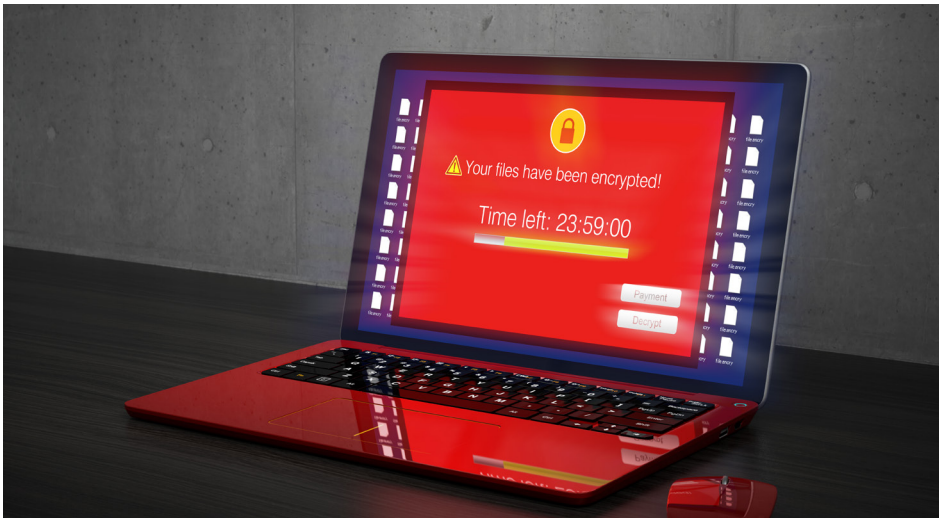
Risikofaktoren:

- Anfällige Software und Systeme
- Keine leicht abrufbaren Backups
- Ineffiziente oder fehlende Cybersicherheit
- Nicht geschulte und anfällige Anwender

Schadenspotenzial:

- Finanzielle Verluste
- Verlust vertraulicher oder proprietärer Daten
- Reputationsschaden
- Unterbrechung der Geschäftsabläufe und Produktivitätsverlust

Der Begriff Ransomware bezieht sich darauf, dass nach der Sperrung der Dateien des Opfers ein Lösegeld (engl. „ransom“) verlangt wird. Diese Malware-Form ist für alle modernen Unternehmen eine große Gefahr und gehört derzeit zu den zerstörerischsten Cyberangriffen. Dabei werden Geschäftsabläufe unterbrochen, Behandlungen in Krankenhäusern unmöglich gemacht und ganze Stadtverwaltungen blockiert. Der beste Schutz vor Ransomware besteht darin, das Eindringen in Ihre Umgebung von Anfang an zu verhindern. Dieses Dokument informiert Sie über diese wachsende Bedrohung.



Bekannt gewordene Ransomware-Angriffe

Universal Health Services verliert 67 Millionen USD durch Ransomware Ryuk
Eine Ransomware-Attacke auf Universal Health Services (UHS) kostete den Gesundheitsdienstleister 67 Millionen US-Dollar durch Ausfälle und damit verbundene Ausgaben. Das Fortune 500-Unternehmen mit einem Jahresumsatz von mehr als 10 Milliarden US-Dollar hat zehntausende Angestellte in den USA und im Vereinigten Königreich.[1]

UCSF zahlt 1,14 Millionen USD Lösegeld für Zugriff auf Forschungsdaten
Den Angreifern gelang es, die IT-Systeme der UCSF School of Medicine zu sperren. Die Administratoren konnten die Infektion jedoch schnell eingrenzen und die betroffenen Systeme isolieren. Dadurch hatte die Ransomware keine Möglichkeit, das innere UCSF-Netzwerk zu erreichen und weitere Schäden zu verursachen.[2]

Cognizant-Umsätze durch Ransomware-Kosten von 50–70 Mio. USD belastet
Der IT-Service-Anbieter Cognizant wurde Anfang April 2020 von einer Ransomware-Attacke getroffen, die die Umsätze des 2. Quartals belastete. Es entstanden Rechtskosten, Beraterkosten sowie weitere Kosten zur Untersuchung des Vorfalls, der Wiederherstellung des Service sowie zur Behebung des Problems.[3]

1 Phil Muncaster (*Infosecurity*): „Universal Health Services Estimates $67 Million in Ransomware Losses“ (Universal Health Services schätzt Ransomware-Verluste auf 67 Mio. USD), März 2021.
2 Charlie Osborne (*ZDNet*): „University of California SF pays ransomware hackers $1.14 million to salvage research“ (University of California San Francisco zahlt Ransomware-Hackern 1,14 Mio. USD, um wieder an Forschungsergebnisse zu gelangen), Juni 2020.
3 Catalin Cimpanu (*ZDNet*): „Cognizant expects to lose between $50m and $70m following ransomware attack“ (Cognizant rechnet nach Ransomware-Angriff mit Verlusten von 50–70 Mio. USD), Mai 2020.

Ransomware-Attacke unterbricht Treibstoffversorgung in den USA

Im Mai 2021 wurde eine der landesweit längsten Pipelines nach einem Ransomware-Angriff gesperrt. Dabei kam das gesamte fast 9.000 Kilometer lange System, das beinahe die Hälfte des Treibstoffbedarfs der amerikanischen Ostküste deckt, vollständig zum Erliegen.[4] Der Pipeline-Betreiber zahlte den Angreifern 4,4 Millionen US-Dollar, um die Daten wieder freizugeben. Doch das genügte letztendlich nicht, um den Betrieb der Pipeline sofort wiederherzustellen.[5]

Weltweit größter Fleischverarbeiter unterbricht Rindfleischproduktion nach Ransomware-Angriff

Das brasilianische Unternehmen musste seine Fleischverarbeitungsbetriebe in Colorado, Iowa, Minnesota, Pennsylvania, Nebraska und Texas nach einem Angriff schließen, der laut US-Behörden aus Russland geführt worden sein soll.[6] In einer Pressemitteilung erklärte das Unternehmen, der Angriff auf seine Computernetzwerke wäre in Nordamerika und Australien entdeckt worden. Die Backup-Server waren jedoch nicht betroffen.[7]

Analyse eines Ransomware-Angriffs

Innerhalb von mehr als dreißig Jahren hat sich Ransomware zu einer der gefährlichsten Cyberbedrohungen entwickelt. Dank digitaler Währungen wie Bitcoin ist es für Cyberkriminelle sehr einfach, an die Lösegelder zu gelangen. Zudem werden die Angreifer immer geschickter darin, veraltete Systeme auszunutzen.

So laufen die meisten Ransomware-Angriffe ab:

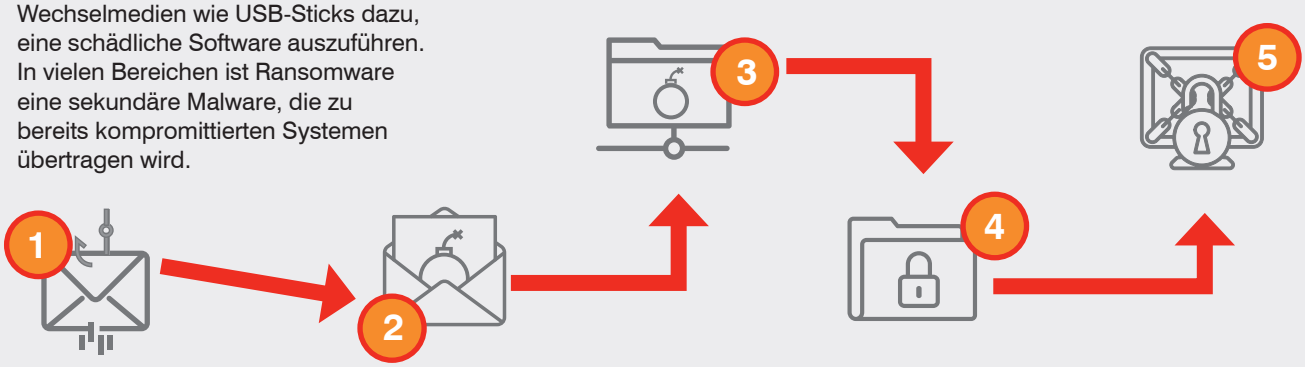
1. Distribution | Angreifer verleiten die Anwender mit Phishing-E-Mails, Social Engineering, gefälschten Websites mit schädlichen Links sowie infizierten Wechselmedien wie USB-Sticks dazu, eine schädliche Software auszuführen. In vielen Bereichen ist Ransomware eine sekundäre Malware, die zu bereits kompromittierten Systemen übertragen wird.

2. Infektion | Der Anwender lädt ahnungslos eine ausführbare Datei herunter (den so genannten Loader bzw. Downloader), der die Ransomware installiert.

3. Staging | Die Ransomware-Schaddaten, die von der Datei abgelegt wurden, verstecken und verankern sich im System.

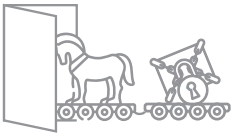
4. Scan und Verschlüsselung | Anschließend scannt die Malware das System sowie das Netzwerk und verschlüsselt die Dateien.

5. Lösegeldforderung | Dem Opfer wird eine Meldung angezeigt, die Lösegeld für die Freigabe der Dateien fordert.



Die Cyberkriminellen mussten auch feststellen, dass die meisten ihrer Opfer über Daten-Backups verfügen und sich daher weigern, auf Lösegeldforderungen einzugehen. Deshalb änderten die Bedrohungsakteure ihre Taktik und setzen nun zunehmend darauf, Dateien zu exfiltrieren und zu verschlüsseln, um anschließend mit der Veröffentlichung der gestohlenen Daten zu drohen. Die Informationen können äußerst vertraulich oder privat sein – und eine Veröffentlichung kann verheerende Folgen haben. Besonders raffinierte Ransomware-Familien finden und verschlüsseln sogar Backups.

4 David E. Sanger, Clifford Krauss und Nicole Perlroth (*The New York Times*): „Cyberattack Forces a Shutdown of a Top U.S. Pipeline“ (Cyberangriff legt wichtige US-Pipeline still), Mai 2021.
5 Collin Eaton und Dustin Volz (*The Wall Street Journal*): „Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom“ (CEO von Colonial Pipeline erklärt, warum er Hackern 4,4 Mio. USD Lösegeld gezahlt hat), Mai 2021.
6 Jacob Bunge (*The Wall Street Journal*): „Meat Buyers Scramble After Cyberattack Hobbles JBS“ (Fleischkäufer alarmiert nach Unterbrechung bei JBS durch Cyberangriff), Juni 2021.
7 Hamza Shaban, Ellen Nakashima und Rachel Lerman (*The Washington Post*): „JBS, world's largest meat processor, shut down U.S. beef plants amid cyberattack“ (Weltgrößter Fleischverarbeiter JBS legt Fleischfabriken nach Cyberangriff still), Juni 2021.



ENTWICKLUNG VON RANSOMWARE-ANGRIFFEN

Ransomware war einstmals die primäre Malware bei schädlichen E-Mail-Kampagnen, zählt mittlerweile jedoch zu den sekundären Infektionen.

Cyberkriminelle, die Trojaner und andere Malware-Typen verteilen, gewähren Ransomware-Gruppen gegen Gewinnbeteiligung Backdoor-Zugriff auf infizierte Systeme.

Für die meisten Unternehmen besteht also der beste Schutz vor Ransomware in der Vermeidung der Erstinfektionen. Mit anderen Worten: Wenn Sie die Loader blockieren, blockieren Sie die Ransomware.

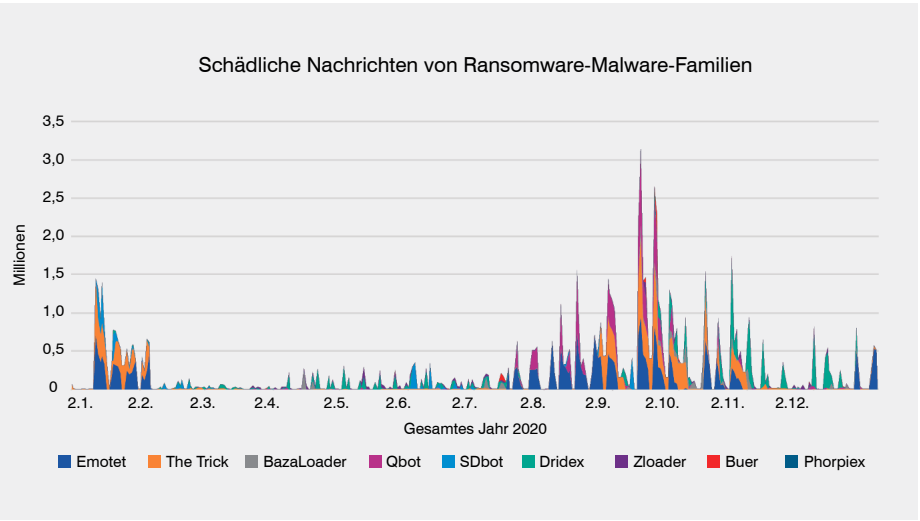
Forschungserkenntnisse

Ransomware wird häufig als Sekundärinfektion übertragen, nachdem ein System bereits durch eine schädliche E-Mail kompromittiert wurde. Viele berüchtigte Malware-Familien, die von uns und anderen Forschern beobachtet werden, sind eng mit nachfolgenden Ransomware-Infektionen verbunden.

Dies ist eine Liste der häufigsten Malware-Familien und der zugehörigen Ransomware:

MALWARE/DOWNLOADER	ZUGEORDNETE RANSOMWARE
Emotet	Ryuk
The Trick	Conti
Dridex	BitPaymer/DoppelPaymer
Qbot	Egregor
SDBbot	Clop
ZLoader	Egregor und Ryuk
Buer (Buer Loader)	Ryuk
Phorpiex/Trik	Avaddon

Emotet, The Trick, Dridex und Qbot gehörten im Jahr 2020 zu den aktivsten Malware-Familien – mit einem gleichmäßig über das Jahr verteilten Aufkommen und einem deutlichen Anstieg im Herbst.



Mehr Organisationen zahlen – mit unterschiedlichem Ergebnis

Laut dem „Proofpoint State of Phish"-Bericht 2021 haben 68 % der befragten US-Organisationen im Jahr 2020 ein Lösegeld gezahlt – das sind doppelt so viele wie der weltweite Durchschnittswert. Im Gegensatz dazu weigerten sich 41 % der spanischen Organisationen, nach einer Infektion das Lösegeld zu zahlen. Weltweit gesehen sind sie damit am seltensten auf die Forderungen der Angreifer eingegangen.

Nach der Zahlung eines einmaligen Lösegeldes konnten 78 % der französischen Organisationen den Zugriff auf ihre Daten wiederherstellen. An zweiter Stelle kamen die USA mit 76 %.

Laut IT-Sicherheitsexperten waren im Jahr 2020 immerhin 34 % der Organisationen infiziert und entschieden sich für die Lösegeldzahlung. 32 % wurden infiziert, zahlten jedoch kein Lösegeld, während bei 34 % keine Ransomware-Infektion auftrat.

So schützen Sie Ihr Unternehmen

Der beste Weg, mit Ransomware fertig zu werden, besteht darin, die Infektion von Anfang an zu verhindern.

Vor dem Angriff

Beginnen Sie mit der Annahme, dass eine Ransomware-Infektion irgendwann erfolgreich sein wird. Sie sollten einen Plan für die Prävention, Erkennung und Reaktion haben. Beispiele:

- Backup wichtiger Daten, Tests von Wiederherstellungsverfahren, Isolierung der Backups von den primären Dateisystemen
- Aktualisieren und Patchen von Systemen
- Schulungen und Weiterbildungen für die Anwender
- Investition in personenzentrierte Sicherheitslösungen
- Netzwerksegmentierung zur Eindämmung der Infektion
- Entscheiden Sie vor dem Angriff, unter welchen Umständen Ihr Unternehmen bereit ist, ein Lösegeld zu zahlen – und wie viel.

Während des Angriffs

Wenn Sie angegriffen werden, sollten Sie weitere Schäden verhindern und einen Reaktionsplan parat haben. Beispiele:

- Anruf an die Strafverfolgungsbehörden
- Abtrennung vom Netzwerk
- Ermittlung des Umfangs des Problems basierend auf Bedrohungsdaten
- Koordination der Gegenmaßnahmen
- Netzwerksegmentierung zur Eindämmung der Infektion
- Suche nach weiteren Schwachstellen, Malware- und System-kompromittierungen im Zusammenhang mit der Ransomware
- Bauen Sie nicht auf kostenlose Ransomware-Entschlüsselungstools
- Stellen Sie wichtige Daten wieder her und suchen Sie dabei nach Malware, die zusammen mit anderen Daten gesichert wurde.

Nach dem Angriff

Nach einem Ransomware-Angriff sollten Sie eine Wiederherstellung durchführen und durch den Vorfall verursachte Probleme lösen. Beispiele:

- Bereinigung und Problembehebung
- Rückschau-Sicherheitsanalysen
- Bewertung des Sicherheitsbewusstseins der Anwender
- Risikobasierte, personenzentrierte Kontrollen
- Neubewertung der Sicherheitslage und Optimierung der Investition mit den größten Risikobereichen

Sollten Sie das Lösegeld zahlen?

Lösegeldzahlungen finanzieren kriminelle Aktivitäten. Die Konsequenzen eines Angriffs können jedoch für das Unternehmen und seine Kunden verheerend sein, sodass die richtige Antwort nicht immer offensichtlich ist.

Vor der Entscheidung für eine bestimmte Vorgehensweise müssen Unternehmen verschiedene Faktoren berücksichtigen:

- Die Sicherheit der Kunden und Mitarbeiter
- Zeit- und Ressourcenaufwand für die Wiederherstellung
- Verantwortung gegenüber den Anteilseignern für das Weiterlaufen des Geschäftsbetriebes
- Kriminelle Aktivitäten, die das Lösegeld finanzieren kann

Ganz gleich, welche Entscheidung getroffen wird, sollte das vor einem Angriff geschehen, wenn den Führungskräften keine unterbrochenen Geschäftsabläufe und Zeitdruck im Nacken sitzen. Dabei sollte nicht nur die Frage geklärt werden, ob das Unternehmen auf die Lösegeld-forderung eingeht, sondern auch wie viel und unter welchen Bedingungen. Berücksichtigen Sie auch, dass einige Zahlungen – zum Beispiel an Angreifer auf US-Sanktionslisten – illegal sein können.

WEITERE INFORMATIONEN

Die beste Möglichkeit zur Abwehr von Ransomware ist proaktiver Schutz. Ein robuster Plan zur Ransomware-Vermeidung umfasst personenzentrierte Sicherheitsmaßnahmen. Dabei ist einer der Aspekte die Sensibilisierung Ihrer Mitarbeiter für reale Angriffstechniken mithilfe von Schulungen. Die Sicherheitsmaßnahmen erkennen und blockieren Ransomware- und Malware-Downloader, die Ihre Mitarbeiter angreifen. Zudem können Sie mithilfe des Plans schnell reagieren und die richtigen Maßnahmen ergreifen, bevor schwerwiegende Schäden auftreten.

Wenn Sie mehr darüber erfahren möchten, wie Sie Ransomware effektiv stoppen können, laden Sie unseren Leitfaden zum Überleben von Ransomware herunter (in englischer Sprache).

Weitere Informationen finden Sie unter **proofpoint.de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

1202-008-01-01 07/21