DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung Ransomware im Unternehmen

So schützen Sie Ihr Business vor Erpressertrojanern

12.01.2022

Ransomware-Angriffe halten die Unternehmenswelt weltweit in Atem. Die Erpressertrojaner befallen ganze Netzwerke und verschlüsseln alle Daten, die sie finden können. Datenbanken, Patientenakten, CAD-Zeichnungen – nichts ist vor der ausgeklügelten Schadsoftware sicher. Aber wie funktioniert Ransomware eigentlich? Auf welchen Wegen gelangt die Bedrohung ins Unternehmensnetzwerk und wie können Sie sich davor schützen?

Was heißt Ransomware?

Der englische Begriff "ransom" bedeutet "Lösegeld", was das Ziel von Ransomware bereits beschreibt. Die Schadsoftware verschlüsselt bei ihrem Angriff wichtige Dateien, macht sie dadurch unbrauchbar und verlangt für die Entschlüsselung die Zahlung einer nicht unerheblichen Geldsumme – meist in Form von Bitcoins, bei denen sich der Geldfluss leichter verschleiern lässt als bei herkömmlichen Währungen. Die Daten werden von der Schadsoftware als Geiseln gehalten und erst gegen die Zahlung eines Lösegelds wieder freigegeben. Aufgrund ihrer Funktionsweise werden diese Schädlinge daher oft auch als "Erpressertrojaner", "Verschlüsselungstrojaner" oder "Kryptotrojaner" bezeichnet.

Berühmte Ransomware-Beispiele im Unternehmensumfeld

Wie funktioniert Ransomware?

Bei Ransomware wird derzeit vor allem zwischen drei Typen unterschieden: **Screenlocker** sind eine harmlosere Variante, die lediglich den Bildschirm des Nutzers sperren und ihm den Zugang zu seinem System verweigern. Sie lassen sich relativ einfach entfernen und richten keinen weiteren Schaden an. **File-Crypter** verschlüsseln Dateien auf der Festplatte, sodass diese ohne den passenden Schlüssel nicht mehr wiederhergestellt werden können. Die gefährlichste Gattung sind sogenannte **Wiper**: Sie verschlüsseln genau wie File-Crypter die Daten auf der Festplatte und verlangen ein Lösegeld – nur ist hier erst gar nicht vorgesehen, dass sie die Daten auch tatsächlich wiederherstellen. Wiper sind darauf programmiert, möglichst viele Daten zu löschen und dadurch maximalen Schaden anzurichten – egal, ob ein Lösegeld gezahlt wurde oder nicht.

Ransomware-Fälle aus dem Jahr 2020 (Beispiele)

- **Februar 2020:** Ein Automobilzulieferer (u. a. für BMW, VW, Audi und Ferrari) wird Opfer eines Ransomware-Angriffs. Die Ransomware "Cl0p" verschlüsselt 130 Server, 600 Clients und Backups.
- **April 2020:** Ein kommunaler Versorger aus Ludwigshafen wird Opfer eines Angriffs mit der Ransomware "Cl0p". Die Verschlüsselung schlug zwar fehl, ein späterer Abfluss von Daten ins Darknet konnte jedoch nicht verhindert werden.

- **Juli 2020:** Die Ransomware "MAZE" verschlüsselt große Teile der IT-Infrastruktur eines börsennotierten Unternehmens aus der Halbleiterindustrie. Die Folge: Alleine in Deutschland waren 750 Mitarbeitende nicht mehr arbeitsfähig.
- **September 2020:** Ein Erpressungstrojaner verschlüsselt 30 Server eines Universitätsklinikums in NRW. Die Klinik-IT wird lahmgelegt, sodass akute Fälle nicht mehr aufgenommen, sondern auf umliegende Krankenhäuser verteilt werden mussten.
- **Oktober 2020:** Ein Computerspielentwickler mit Sitz in Frankfurt am Main stellt fest, dass seine gesamte Windows-Infrastruktur durch die Ransomware "Egregor" gekapert und verschlüsselt wurde. Da das Unternehmen Lösegeldforderungen nicht erfüllte, wurden interne Daten schrittweise veröffentlicht.
- **Dezember 2020:** Am 12. Dezember 2020 wurde ein Angriff auf ein börsennotiertes Lebensmittel- und Kosmetikunternehmen festgestellt. Große Teile der weltweiten IT-Systeme wurden verschlüsselt. Es folgte ein Produktionsstopp, der das Unternehmenen mehrere Millionen Euro kostete – pro Tag. Die Ursache war ein Angriff mit der Ransomware "Cl0p".

Quelle: Bundeskriminalamt

Vorsicht bei E-Mail-Anhängen

Ransomware kommt meist per E-Mail: Oft verschicken die Erpresser E-Mails mit einem schädlichen Anhang. Der Schädling tarnt sich beispielsweise als Excel-Tabelle mit Makros oder als EXE-Datei, die wie ein harmloses ZIP-Archiv aussieht. Öffnet der User die Datei, installiert er damit unwissentlich auch den Trojaner. Spätestens beim nächsten Neustart beginnt der Trojaner damit, die Dateien auf der Festplatte des Computers sowie allen angeschlossenen Laufwerken zu verschlüsseln.

Einige Vertreter (wie zum Beispiel WannaCry) funktionieren zusätzlich wie ein Wurm und versuchen, über das Netzwerk andere Rechner zu infizieren. Bemerkenswert ist, dass die Erpresser teilweise sehr geschickt vorgehen: So hatte es der 2016 grassierende Schädling "GoldenEye" auf Personalabteilungen in Deutschland abgesehen. Die E-Mails waren in einwandfreiem Deutsch verfasst und bezogen sich auf tatsächliche Stellenausschreibungen des Unternehmens. Selbst vorsichtige Mitarbeiter in der Personalabteilung öffneten daher die angehängten Dateien und infizierten so ihre Rechner.

Auf dem Bildschirm der betroffenen Clients erscheint dann nur noch eine Lösegeldforderung, die verspricht, die Daten gegen Bezahlung wieder zu entschlüsseln. Dafür soll der Nutzer eine individuelle Seriennummer eingeben, die er auf Webseiten im Tor-Netzwerk gegen Bitcoins kaufen kann. Um der Forderung Nachdruck zu verleihen, werden oft alle paar Stunden einige Dateien gelöscht, bis schließlich keine Daten mehr übrig sind. Meist verteuert sich genauso regelmäßig die Seriennummer, um den Nutzer zu einem schnellen Handeln zu zwingen.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Die

Ransomware Petya durchläuft mehrere Phasen, um die Daten des Nutzers zu verschlüsseln und den Rechner unbrauchbar zu machen

Wie erhöhe ich den Ransomware-Schutz in meinem Unternehmen?

- **Legen Sie regelmäßig Backups an**

  Sichern Sie die Daten aller Clients regelmäßig auf Netzlaufwerken, externen Festplatten oder in der Cloud. Achtung: Stellen Sie sicher, dass die Verbindung zu dem Speichermedium oder Netzlaufwerk nach jedem Backup getrennt wird – es droht sonst eine Verschlüsselung aller Backups!

- **Installieren Sie Updates und Patches**

  Halten Sie Software wie das Betriebssystem, den Browser und Plug-ins stets auf dem aktuellen Stand. Sicherheitslücken in Programmen auszunutzen ist eine der beliebtesten Methoden von Cyberkriminellen. Ein zentrales Patch Management hilft Ihnen, die Software auf all Ihren Clients aktuell zu halten und Schadsoftware so möglichst wenig Angriffsfläche zu bieten.

- **Seien Sie vorsichtig bei E-Mails und Links**

  Ein gesundes Misstrauen schadet nicht. Die E-Mail in Ihrem Posteingang ist voller Tippfehler? Oder verspricht Ihnen viel Geld, ohne dass Sie dafür etwas tun müssen? Sie kennen den Absender nicht? Löschen Sie verdächtige E-Mails sofort, ohne sie zu öffnen. Getarnt als Rechnungen, Bewerbungsunterlagen oder als Link zu einer interessanten Website versteckt sich der Schädling im Anhang. Besondere Vorsicht ist geboten bei ausführbaren EXE-Dateien sowie Office-Dokumenten, die mit Makros versehen sind. Am besten verhindern Sie die automatische Ausführung vom Makros in den Office-Suiten aller Clients.

  G DATA Sicherheitslösungen bieten einen speziellen Spamschutz mit OutbreakShield-Technologie. Dieser Schutz erkennt schädliche E-Mails noch bevor sie vom E-Mail-Programm auf den Computer geladen werden. So wird die E-Mail mit den schädlichen Inhalten erst gar nicht zugestellt oder direkt aus dem Postfach entfernt.

- **Schulen Sie Ihre Mitarbeiter mit Security Awareness Trainings**

  Knapp die Hälfte aller Cyberangriffe nutzt den Menschen vor dem Computer als Einfallstor aus. Deshalb wird es für Unternehmen in Zukunft immer wichtiger, Mitarbeiterinnen und Mitarbeiter für die Gefahren durch Cybercrime zu sensibilisieren. In speziellen Security Awareness Trainings lernen sie vorsichtig zu sein und potenziell gefährliche Dateien und Vorgänge als solche zu erkennen.

- **Verwenden Sie eine aktuelle Sicherheitslösung**

  Ransomware ist eine Art von **Malware.** Virenscanner und Verhaltensüberwachung erkennen bekannte Schädlinge wie WannaCry, bevor diese Schaden anrichten können. Ein

zusätzlicher Schutz vor Exploits können die Infektion ebenfalls verhindern. Oft werden Schadprogramme auch an universellen Codeabfolgen erkannt, die typisch sind für Kompression, Verschlüsselung, Downloadroutinen, Backdoor-Aktivitäten, Tarnmechanismen oder dergleichen. Heuristische und generische Signaturen erkennen solche allgemeingültigen Befehlssequenzen auch bei bislang unbekannten Malware-Familien.

Doch Ransomware verbreitet sich nicht nur per E-Mail - sondern auch über **Webseiten** oder andere Internetdienste ("Drive-by-Attacken"). G DATA Sicherheitslösungen arbeiten mit der URL-Cloud, die eine ständig aktualisierte Liste von Webseiten vorhält, die kompromittiert wurden und nun Rechner unbemerkt mit Schadsoftware versorgen. Wenn eine Seite als schädlich markiert wurde, wird der Zugang blockiert. Außerdem überprüft die G DATA Software alle im Browser eingehenden Daten auf Schadcode – seien es Dateidownloads oder aktive Skripte in der Webseite.

Zahlen Sie auf keinen Fall Lösegeld!

Zahlen Sie auf keinen Fall Lösegeld!

Auch wenn Sie das geforderte Lösegeld aufbringen, erhalten Sie im Gegenzug nur selten einen funktionierenden Key zur Entschlüsselung. Bei sogenannten "Wipern" sind Ihre Daten in jedem Fall verloren, selbst wenn Sie das Lösegeld bezahlt haben – hier ist es technisch erst gar nicht vorgesehen, dass die Daten auch wieder entschlüsselt werden können. Signalisieren Sie Zahlungsbereitschaft, nutzt es der Erpresser zudem vielleicht aus und verschlüsselt Ihre Dateien erneut, indem er gut versteckte Teile der Schadsoftware nach einer Weile reaktiviert und erneut Geld fordert. Ganz abgesehen davon, dass die Masche für die Erpresser durch die zahlenden Opfer lukrativ bleibt, was immer wieder Nachahmer mit neuer Schadsoftware auf den Plan rufen wird.

Das ist zu tun, wenn das Netzwerk infiziert wurde

Ist Ihr Netzwerk trotz aller Vorsichtsmaßnahmen durch einen Cyberangriff von Ransomware befallen, sollten Sie die betroffenen Clients oder Server sofort isolieren. Kappen Sie alle Netzwerkverbindungen (am besten physikalisch), damit sich der Schädling nicht weiter ausbreiten kann. Setzen Sie dann die infizierten Rechner zurück und spielen Sie das jeweils letzte Backup ein. Scannen Sie alle anderen Clients und Server im Netzwerk mit einer zuverlässigen Sicherheitslösung, um eine Infektion auszuschließen. Dieser Schritt ist sehr wichtig: Manche Schädlinge verstecken sich im Betriebssystem, um erst zu einem späteren Zeitpunkt zuzuschlagen – ein auf den ersten Blick "sauberer" Client kann also durchaus von Schadsoftware befallen sein.

Falls Sie kein aktuelles Backup des befallenen Clients oder Servers haben, sind Ihre Daten dennoch nicht zwingend verloren: Vor allem für ältere Ransomwares gibt es oft bereits ein Gegenmittel. Versierte Sicherheitsexperten haben die Verschlüsselungsroutinen vieler Schädlinge geknackt und Programme entwickelt, die die Daten wieder entschlüsseln und die Ransomware unschädlich machen können. Schauen Sie im Internet nach entsprechenden Tools, die meist nach dem Schema "XY Decrypter" oder ähnlich benannt sind.

Ist die Situation komplexer oder helfen die herkömmlichen Methoden nicht weiter, bietet sich eine professionelle Beratung durch einen erfahrenen Dienstleister aus dem Bereich IT Security an. Die Experten der G DATA Advanced Analytics bieten zum Beispiel nicht nur Erste Hilfe bei Sicherheitsvorfällen ("Incident Response"), sondern auch Maßnahmen zur Datenrettung sowie eine tiefgehende Malware-Analyse an. So können Sie nach einer Infektion sicher gehen, dass der Schädling sich nicht tief in den Systemen verbirgt und zu einem späteren Zeitpunkt erneut

Quelle: https://www.gdata.de/tipps-tricks/unternehmen-vor-ransomware-schuetzen?utm_source=gd&utm_medium=email&utm_campaign=nl-b2b-sonder-01-22-CIZ-Teil1-Ransomware-de