# Dreifach gestraft: erst Ransomware-Erpressung, dann Datenverlust und zu guter Letzt die Strafgebühr für einen mangelhaften Wiederherstellungsplan. Wie komplex Ransomware in Unternehmensressourcen eingreift.

Im letzten Jahr wurde ein US-Unternehmen, das Treibstoff fördert, von einer Ransomware in die Knie gezwungen. Dahinter steckten kriminelle „Partnerunternehmen“ der berüchtigten DarkSide-Gruppe. Ein typisches Beispiel eines RaaS (Ransomware as a Service)-Angriffs: ein kleines Kernteam von Kriminellen entwickelt eine Schadsoftware, stellt diese anderen Bösewichtern zur Verfügung und kümmert sich um die Lösegelder der Opfer. Jedoch führen sie die tatsächliche Attacke auf das Netzwerk, bei der die Malware ausgeliefert wird, nicht aus. Das übernehmen deren „Partner in crime“, quasi die Außendienstmitarbeiter. In der Regel erhalten sie als Gegenleistung den Löwenanteil des von den Opfern erpressten Geldes.

**RaaS – so funktioniert das Co-Working der Kriminellen**
Die Kerngruppe lauert derweil kaum sichtbar im Hintergrund und betreibt eine Art Franchise-Betrieb, bei dem sie üblicherweise 30 Prozent (nach eigenen Angaben) jeder Zahlung in die eigene Tasche steckt.

Das Team an der Frontlinie geht normalerweise so vor:

- Erkundigungen einholen, um potenzielle Ziele zu finden, in die sie einbrechen können.
- Einbruch in ausgewählte Unternehmen mit ihnen bekannten Schwachstellen.
- Durchsuchen des Netzwerks bis sie administrative Rechte erhalten, um auf das Niveau von offiziellen Administratoren zu gelangen.
- Abbilden des gesamten Netzwerks, um jeden einzelnen Desktop-PC und die Server-Systeme zu finden.
- Lokalisieren und oft auch Neutralisieren existierender Backups.
- Exfiltrieren vertraulicher Firmendaten für ein extra Druckmittel bei der Erpressung.
- Netzwerk-Hintertüren für einen schnellen Rückzug vorbereiten, falls die Angreifer auffliegen.
- Vorsichtiges Prüfen der bestehenden Malware-Verteidigung, Ausschau halten nach schwachen oder ungeschützten Punkten.
- Ausschalten oder zumindest Reduzieren der Sicherheitseinstellungen, die im Weg sind.
- Auswahl einer für das Unternehmen besonders „unangenehmen“ Tageszeit sprich am Wochenende oder nachts.

Und dann setzen die Cyberkriminellen den Ransomware-Code frei, mit dem sie vom Drahtzieher im Hintergrund versorgt wurden. Die Verschlüsselung (nahezu) aller Computer im Netzwerk dauert dann nur wenige Minuten.

**Zur Kasse bitte!**
Die Idee hinter dieser Art von Angriff, liegt darin, dass die Computer nicht vollständig gelöscht werden. In der Tat ist es so, dass nach den meisten Ransomware-Angriffen die Betriebssysteme weiterhin hochfahren und die primären Anwendungen auf den Computern laden, um den Anschein zu wahren, dass alles normal sei.

Das Opfer kann seinen Laptop hochfahren, Word laden, sämtliche Dokumente in den Verzeichnissen sehen, sogar versuchen, sie zu öffnen, wird dann aber das digitale Äquivalent eines geschredderten Weißkohls zu sehen bekommen. Die Daten sind verschlüsselt und es existiert nur eine Kopie des Dechiffrier-Schlüssels – und den haben die Angreifer. Das ist der Zeitpunkt, an dem meistens die „Verhandlungen“ beginnen. Dabei bauen die Kriminellen darauf, dass die IT-Infrastruktur des Opfers durch die verschlüsselten Daten so stark beeinträchtigt ist, dass sie nicht mehr funktionsfähig ist, und das Opfer somit bereit ist, ein Lösegeld zu bezahlen.

„Zahlt uns eine ‚Wiederherstellungsgebühr' und wir werden euch die Entschlüsselungs-Werkzeuge liefern, um sämtliche Computer wieder nutzbar zu machen - und wir ersparen euch die Zeit, die ihr für die Wiederherstellung aus Backups benötigt. Sofern ihr überhaupt funktionierende Backups habt.“ So oder so ähnlich klingen die Forderungen, wie sie beispielsweise auch beim US-Unternehmen vor rund 12 Monaten eintrafen.

Auch wenn Strafverfolgungsbehörden weltweit Ransomware-Opfer mahnen, nichts zu bezahlen (und wir mittlerweile wissen, dass heutige Ransomware-Zahlungen unmittelbar morgige Ransomware-Angriffe finanzieren), entschied sich das Unternehmen in diesem Beispiel, die geforderten rund 4,4 Millionen US-Dollar in Bitcoins zu überweisen.

Der diesjährige Sophos Ransomware-Report State of Ransomware 2022 enthüllt, dass nur 4% der Zahler weltweit sämtliche Daten zurückerhalten. Im Durchschnitt bekommt man nur zwei Drittel (genau: 60,56%). In Deutschland liegt der Anteil bei 64%. Aus weltweiter Sicht liegt dieser Wert bei Betrieben der Energieversorgung nur geringfügig höher mit 62% (genau: 61,59%). Das bedeutet: Zahlt ein Unternehmen das Lösegeld, hat es dennoch sehr hohe Verluste an Daten hinzunehmen. Keinesfalls ist damit der Fall erledigt.

**Nach Lösegeld kam die Strafgebühr**

Auf den Pipeline-Betreiber kam nun auch ein behördlicher Appell zu: Das US-Department of Transportation brummte dem Betrieb eine Zivilstrafe von 986.400 US-Dollar auf, das Resultat einer Untersuchung durch die Pipeline and Hazardous Materials Safety Administration (PHMSA). Der Check lief zwischen Januar und November 2020 also in dem Jahr BEVOR die Ransomware-Attacke stattfand. Die Probleme, die das Institut identifizierte, existierten also und waren bekannt. Die PHMSA legte dar, dass die primären operationalen Mängel, die für mehr als 85 Prozent der Gebühr verantwortlich sind (846,300 US-Dollar) „ein wahrscheinliches Versäumnis sind, die manuelle Abschaltung und Wiederinbetriebnahme seines Pipelinesystems angemessen zu planen und vorzubereiten“. Und sie behauptet, dass diese Versäumnisse „zu den nationalen Auswirkungen beitrugen, als die Pipeline nach dem Cyberangriff im Mai 2021 außer Betrieb blieb."

**Einzelfall oder Handlungsempfehlung für jeden?**

Das klingt zunächst wie ein außergewöhnlicher Fall, denn wer betreibt schon eine Pipeline, und dann auch noch in dieser Dimension. Dennoch werden in der offiziellen PHMSA-Mitteilung über einen wahrscheinlichen Verstoß einige damit zusammenhängende Probleme genannt, aus denen alle lernen können:

Bei dem Pipeline-Betreiber lagen die Probleme in internen Bereichen des Unternehmens, wie Überwachungssteuerung und Datenerfassung, industrielle Steuerungssysteme und Betriebstechnologie, das so genannte SCADA (Supervisory Control and Data Akquisition): Computersystem, das technische Prozesse automatisiert überwacht sowie steuert und von Energieversorgern bis hin zu Flughäfen im Einsatz ist. Auch ICS (ein Akronym für Industrial Control Systems) und OT (Operational Technology) waren mangelhaft. OT lässt sich als industrieller Gegenpart zur IT begreifen, aber die SecOps (Security Operations) sind für beide Arten eine ähnliche Herausforderung.

Auch wenn die Betriebstechnologie und IT-Funktionen wie zwei separate Netzwerke erscheinen, die möglichen Konsequenzen von SecOps-Fehlern in dem einen Bereich können direkt und sogar gefährlich den anderen Bereich beeinflussen.

Noch wichtiger, vor allem für viele kleinere Unternehmen, ist, dass selbst wenn keine Pipeline, kein Stromversorgungsnetz oder kein Kraftwerk betrieben wird, höchstwahrscheinlich trotzdem eine Art Betriebstechnik-Netzwerk im Einsatz ist, das aus IoT-Geräten wie Sicherheitskameras, Türschlössern, Bewegungssensoren und vielleicht sogar einem beruhigend wirkenden, computergesteuerten Aquarium im Empfangsbereich besteht.
Und diese werden meist im gleichen Netzwerk betrieben, in dem sich auch das gesamte IT-System befindet. Die Cybersicherheitsmaßnahmen beider Gerätetypen sind also untrennbar miteinander verwoben.

**Fünf Punkte, die jedes Unternehmen ernst nehmen sollte**
Der PHMSA-Bericht listet Probleme auf, die alle unter den Sammelbegriff Kontrollraummanagement fallen, das man sich als das Betriebstechnologie-Äquivalent zum Network Operations Centre einer IT-Abteilung vorstellen kann (oder einfach als „das IT-Team" in einem kleinen Unternehmen).

Zusammengefasst geht es um diese fünf Probleme:
1. Versäumnis, eine ordnungsgemäße Aufzeichnung über bestandene Betriebstests zu führen.
2. Versäumnis, die Funktion von Alarm- und Anomaliedetektoren zu testen und zu überprüfen.
3. Kein Notfallplan für die manuelle Wiederherstellung und den Betrieb im Falle eines Systemausfalls.
4. Versäumen der Tests der Backup-Prozesse und -Prozeduren.
5. Mangelhaftes Reporting von fehlenden oder vorübergehend unterdrückten Sicherheitskontrollen.

**Was können wir für unsere IT-Sicherheit daraus lernen?**
Jedes der oben genannten Versäumnisse kann versehentlich auftreten. Laut Sophos Ransomware Report 2022 gaben zwei Drittel (genau: 66%) der Befragten an, im vorigen Jahr Opfer eines Ransomware-Angriffs geworden zu sein. Der Energieversorgungs-Sektor lag mit 75% sogar deutlich über dem Durchschnitt. Bei rund zwei Dritteln davon wurden die Daten verschlüsselt und die Hälfte von ihnen verhandelte mit den Kriminellen.
Das suggeriert, dass ein signifikanter Anteil (etwas mehr als jeder Fünfte) der IT oder SecOps Teams in einer oder mehreren der oben genannten Kategorien die Übersicht verloren hat.
Dazu gehören die Punkte 1 und 2 (Sind Sie sicher, dass die Sicherung tatsächlich funktioniert hat? Haben Sie dies formell festgehalten?), Punkt 3 (Was ist Ihr Plan B, wenn die Kriminellen Ihre primäre Sicherung löschen?), Punkt 4 (Haben Sie die Wiederherstellung so sorgfältig geübt, wie Sie sich um die Sicherung gekümmert haben?) und Punkt 5 (Sind Sie sicher, dass Sie nichts übersehen haben, auf das Sie damals hätten aufmerksam machen sollen?).

Für viele IT-Teams oder gerade auch für kleinere Betriebe, die IT „nebenbei“ erledigen, ist ein spezialisiertes SecOps-Team ein Luxus und schlichtweg nicht bezahlbar, so dass die Strategie dort oft einem „Installieren und dann Vergessen“-Prinzip gleichkommt. Wer sich in dieser Situation befindet, sollte sich von externen MTR-Experten unterstützen lassen und diese als eine Investition in die sicherere Zukunft ansehen.
Cybersecurity ist ein Prozess, kein Ziel. Ein erfolgreicher Angriff hinterlässt immer einen Schaden und hat Nachwirkungen auf Ressourcen und Betriebsfähigkeit. Die Stärke des Einschlages hängt dabei stark von Reaktionsschnelligkeit, Vorsorge und angelegtem Sicherheitsprozess ab.

**Social Media von Sophos für die Presse**
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

**Pressekontakt:**

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de