Fortschrittliche Angriffe

Neue Qualität aktueller Angriffe und Prognose

Ausgangslage

Seit der großflächigen Verbreitung von „Locky“ in 2016 hat der Einsatz von Erpressungs-Schadsoftware mit Verschlüsselungsfunktion – sogenannte Crypto-Ransomware – in den beobachteten und gemeldeten Cybercrime-Fällen weiter deutlich zugenommen. Dabei werden die IT-Systeme der Betroffenen durch eine Verschlüsselung beeinträchtigt, ihre Verfügbarkeit erheblich eingeschränkt und die Besitzer mit einer Aufforderung zur Zahlung eines Lösegelds für die Entschlüsselung der Daten erpresst. Diese Methode ist durch die Sichtbarkeit und unmittelbare Wirksamkeit besonders effektiv. Bei diesem Vorgehen nutzen die Täter Fehler des Betroffenen wie Fehlbedienung, Fehlkonfigurationen, veraltete Software-Stände oder mangelhafte Datensicherungen aus. Die Zahlung des Lösegelds wird meist in elektronischen Währungen (üblicherweise Bitcoin) gefordert. Dies ist für die Täter im Vergleich zum „klassischen“ Betrug beim Online-Banking deutlich einfacher, schneller und kostengünstiger – und somit attraktiver.

Angriffselemente

Der zunehmende Einsatz von Ransomware bei Cybercrime-Angriffen geht einher mit stark verbesserten Angriffsmethoden und ständig angepassten Vorgehensweisen der Täter, die in einer signifikanten qualitativen Steigerung der Bedrohungslage münden. Dabei wurden bereits Unternehmen und Organisationen jeder Größe und Branche weltweit zu Opfern. Neben Konzernen waren in Deutschland so auch zahlreiche kleine und mittelständische Unternehmen, Krankenhäuser, Universitäten, kommunale Verwaltungen und Privatanwender betroffen. Erschwerend kommt durch die Anfang 2020 aufgetretene COVID-19-Pandemie für viele Organisationen ein wirtschaftlicher und finanzieller Ausnahmezustand hinzu, der eine unter normalen Umständen mögliche Erholung von einem derartigen Angriff stark hemmt oder gar unmöglich macht.

Ausgefeiltes Social Engineering

Die Täter nutzen wirksame „Social Engineering“-Techniken zur Verbreitung von Schadsoftware. Dabei werden nicht nur Absenderadressen von E-Mails gefälscht, sondern vermeintliche Antworten auf zuvor ausgespähte E-Mails an die Kommunikationspartner versendet. Die bekannten Betreffzeilen und zitierten E-Mail-Inhalte tatsächlicher vorausgegangener Kommunikation lassen die Spam-Mails für die Empfänger authentisch erscheinen und verleiten sie dazu, die angehängten schädlichen „Köder“-Dokumente zu öffnen und die Ausführung aktiver Inhalte freizugeben. Dies führt zu einer erhöhten Durchschlagsquote dieser Angriffe. Entsprechendes Vorgehen wird bei mehreren Angreifergruppen beobachtet.

<u>Mögliche Schadenswirkung durch Arbeits-/ Produktionseinschränkungen bzw. -ausfall bei einer Infektion einzelner Arbeitsplätze:</u>

Bei Einzelplatzinfektionen können durch geeignete und schnelle Maßnahmen möglicherweise die weitergehende Übernahme des Netzwerks durch die Täter und eine Verschlüsselung verhindert werden, sofern die Infektion frühzeitig erkannt wird. Allerdings kann hierbei durch eine unsachgemäße Vorgehensweise bei der Bereinigung die Situation auch schnell verschlimmert werden. Schadsoftware verfügt häufig zudem über ausgeklügelte Gegenmaßnahmen, die einer Sicherheitssoftware die Erkennung erschwert.

Auswirkung: Ausfall der Arbeitsfähigkeit einzelner Mitarbeiter von einigen Stunden bis wenigen Tagen.

Prognose: Tendenz weiter zunehmend

Ausgefeilte Social-Engineering-Methoden werden durch viele weitere Tätergruppen aufgegriffen, eingesetzt (vgl. z. B. QakBot) und weiter verbessert.

Hochwertige Angriffstechniken

Nach einer initialen Infektion wird in der Regel weitere Schadsoftware nachgeladen, z. B: Trickbot. Hierbei handelt es sich um eine fortschrittliche Schadsoftware, die verschiedene Werkzeuge und Methoden nutzt, um automatisiert das Netzwerk des Betroffenen – bis hinein in die zentralen Komponenten der Nutzerrechteverwaltung (Active Directory) – komplett zu übernehmen. Damit ist das Unternehmensnetz häufig vollständig kompromittiert und nicht mehr vertrauenswürdig. Der Angreifer besitzt anschließend alle Rechte, um beispielsweise Benutzerkonten mit Administrator-Rechten anzulegen, Daten einzusehen und abfließen zu lassen oder Hintertüren einzurichten. Damit nutzt jetzt auch weit verbreitete Crime-Schadsoftware flächig, standardmäßig und automatisiert Techniken, die zuvor nur im Zusammenhang mit zielgerichteten Spionage-Angriffen beobachtet wurden. Dies stellt eine neue Dimension der Bedrohungslage insbesondere für kleine und mittelständische Unternehmen dar, die bislang von fortschrittlichen hochwertigen Angriffstechniken nicht unmittelbar bedroht waren. Diese Bedrohung gilt gleichermaßen auch für Betreiber Kritischer Infrastrukturen wie Krankenhäuser, Behörden aller föderalen Ebenen und weitere Organisationen.

Mögliche Schadenswirkung durch Arbeits-/ Produktionseinschränkungen bzw. -ausfall bei einer vollständigen Übernahme des Netzwerks:

Erfolgt eine vollständige Übernahme des Netzwerks durch die Täter, muss dieses komplett parallel neu aufgebaut werden, um wieder eine vertrauenswürdige Umgebung zu schaffen.

Auswirkung: Beeinträchtigung der Arbeitsfähigkeit von mehreren Tagen bis wenigen Wochen, davon ggf. zeitweise kompletter Ausfall.

Prognose: Tendenz zunehmend

Die Methode wird durch viele weitere Tätergruppen aufgegriffen, eingesetzt und weiter verbessert. Derart leicht automatisiert vollständig übernommene Netze lassen sich vielfältig missbrauchen.

Automatisierte und manuelle Aufklärung von Netzwerken

Während der automatisierten Ausbreitung späht das Schadprogramm das Netzwerk des Opfers aus und übermittelt die dabei gesammelten Informationen über Systeme, Benutzer und installierte Software an die Täter. Auf Basis dieser Informationen entscheiden die Täter, ob es sich bei dem Opfer um ein „lohnendes“ Ziel handelt, das eine weitere manuelle „Bearbeitung“ verdient. Erachten die Täter ein Opfer als ausreichend interessant, verbinden sie sich über den von Trickbot bereitgestellten Fernzugriff auf dessen Systeme, schauen sich manuell im Netzwerk um und ziehen dabei ggf. weitere interne Informationen ab. Dies erfolgt häufig erst zwei bis drei Wochen nach der Erstinfektion, da die Täter vermutlich aufgrund der Vielzahl weltweiter Opfer ein großes „Angebot“ abzuarbeiten haben.

Mögliche Schadenswirkung durch Arbeits-/ Produktionseinschränkungen bzw. -ausfall bei einer manuellen Aufklärung des Netzwerks:

Erfolgt eine manuelle Aufklärung des Netzwerks ggf. mit weiteren Angriffstools durch die Täter, muss dieses umfangreich forensisch untersucht und komplett parallel neu aufgebaut werden, um wieder eine vertrauenswürdige Umgebung zu schaffen.

Auswirkung: Beeinträchtigung der Arbeitsfähigkeit von wenigen bis einigen Wochen, davon ggf. zeitweise kompletter Ausfall.

Prognose: Tendenz zunehmend

Die manuelle Aufklärung wird durch wenige Tätergruppen eingesetzt und weiter verbessert. Da die verfügbaren Kapazitäten für eine manuelle Aufklärung wegen der erforderlichen Kompetenzen begrenzt sind, wird sie überwiegend bei erfolgversprechenden Hochwertzielen eingesetzt.

Verschlüsselung von Systemen

Stellen die Täter fest, dass sie mit einer Verschlüsselung von Daten große Teile der Organisation lahmlegen könnten und es sich um ein zahlungskräftiges Unternehmen handelt, das potenziell bereit ist, ein hohes Lösegeld für die Entschlüsselung zu bezahlen, rollen sie Ransomware wie Ryuk gleichzeitig auf allen (Server-) Systemen aus. Dabei werden aufgrund der dem Angreifer zur Verfügung stehenden hohen Rechte oder nicht ausreichend durchdachter Backup-Konzepte häufig auch alle Datensicherungen verschlüsselt, sofern diese nicht offline gehalten werden. Die Lösegeldforderungen bewegen sich häufig im sechsstelligen Euro-Bereich, dem BSI sind aber auch achtstellige Lösegeldforderungen bekannt.

Mögliche Schadenswirkung durch Arbeits-/ Produktionseinschränkungen bzw. -ausfall bei verfügbaren Datensicherungen:

Findet zusätzlich eine Verschlüsselung statt, aber es sind integre aktuelle Datensicherungen verfügbar, müssen diese nach der Bereinigung des Netzwerks zurückgespielt werden, um die Daten wieder nutzen zu können. Die „verlorene Zeit“ muss nachgearbeitet werden.

Auswirkung: Beeinträchtigung der Arbeitsfähigkeit von mehreren Tagen bis einigen Wochen, davon ggf. zeitweise kompletter Ausfall.

Mögliche Schadenswirkung durch Arbeits-/ Produktionseinschränkungen bzw. -ausfall bei nicht-verfügbaren Datensicherungen:

Wurden auch alle aktuellen Datensicherungen vernichtet, bleibt oft nur die Rekonstruktion vereinzelter alter, unvollständiger Einzelsicherungen und viel manuelle Nacharbeit.

Auswirkung: Beeinträchtigung der Arbeitsfähigkeit von mehreren Wochen bis Monaten. Dieser Fall kann insbesondere für kleinere Unternehmen existenzbedrohend sein.

Prognose: Tendenz gleichbleibend

Die Methode wird durch viele Tätergruppen eingesetzt und weiter verbessert. Die Zahl der verschiedenen Ransomware-Arten wird weiter zunehmen. Allerdings stellen sich viele Unternehmen durch bessere Sicherung der Backups darauf ein und schränken die Wirksamkeit der Methode teilweise ein.

Abfluss und Veröffentlichung von Daten

Verschiedene Tätergruppen sind dazu übergegangen, vor der Verschlüsselung auch Daten aus dem Netzwerk Betroffener auszuleiten und drohen mit einer Veröffentlichung dieser Daten, falls Betroffene die Zahlung des geforderten Lösegelds verweigern. Da sich für Betroffene aus einer Veröffentlichung unter Umständen ein Reputationsverlust und weitere negative finanzielle Auswirkungen ergeben würden, steigern die Täter hiermit

den Handlungsdruck bei den Betroffenen hin zu einer Zahlung des Lösegelds. Des Weiteren besteht bei einer Erpressung im Kontext der Verschlüsselung von infizierten Systemen somit weiterhin ein Handlungsdruck, auch wenn die Wiederherstellung von Daten mittels Backups sichergestellt ist. Auch von deutschen Betroffenen wurden bereits mehrfach Daten veröffentlicht. Es muss davon ausgegangen werden, dass derartige Angriffe auch zukünftig von Datenabflüssen und verstärkt auch mit Androhungen einer Veröffentlichung der Daten begleitet werden. Teilweise wurden auch direkt Kunden mit den abgeflossenen Daten erpresst.

Mögliche Schadenswirkung durch Arbeits-/ Produktionseinschränkungen bzw. -ausfall bei Abfluss von Daten:

Bei Tätergruppen, die Daten erfolgreich verschlüsseln konnten, muss davon ausgegangen werden, dass sie auch in der Lage waren, zuvor Daten aus dem Netzwerk auszuleiten. Die Daten können in der Folge für weitere Angriffe oder zur erpresserischen Ansprache ihrer Partner herangezogen oder ggf. medienwirksam offengelegt werden.

Auswirkung: Reputationsverlust und negative finanzielle Auswirkungen.

Prognose: Tendenz weiter zunehmend

Die Methode wird durch viele weitere Tätergruppen aufgegriffen, eingesetzt und weiter verbessert. Es wird in den nächsten Monaten darauf ankommen, wie betroffene Unternehmen kommunikativ gegenüber den Medien, Zulieferern und Kunden mit der Erpressung umgehen und wie die Medien derartige Vorfälle aufgreifen. Dies wird entscheiden, ob sich diese Art der „Vertraulichkeits"-Erpressung gegenüber der effektiveren „Verfügbarkeits"-Erpressung wirtschaftlich für die Täter auszahlt und bestimmt die langfristige Tendenz der Einsatzhäufigkeit.

Essentielle Vorsorgemaßnahmen

- Sicherheitskonzepte und Notfallpläne erstellen und regelmäßig überprüfen,
- Netzwerk-Segmentierung und strikte Rechte-Trennung im Active Directory, um eine ungehemmte Ausbreitung von Schadprogrammen und vollständige Kompromittierung des Netzwerks zu verhindern,
- vollständige Backup-Strategie inkl. Offline-Backups (auch regelmäßig Wiederherstellung prüfen),
- Patch-Management verifizieren – insbesondere Sicherheitsupdates für kritische Schwachstellen müssen zeitnah ausgerollt werden,
- Logging-Strategie umsetzen, über die ein Abfluss von Daten nachvollzogen werden kann,
- Sensibilisierung von Mitarbeitern und Umsetzung technischer Maßnahmen zur Härtung von (Arbeitsplatz-)Systemen müssen Hand in Hand gehen,
- Maßnahmen entwickeln, wie mit einem Abfluss und einer Offenlegung unterschiedlicher auch sensibler Daten umgegangen werden kann sowie
- Management-Awareness schaffen, um Cyber-Risiken als Bestandteil des Risiko- und Vorsorgemanagements zu verankern.

Diese Aufzählung ist nicht vollständig und ersetzt nicht die Umsetzung des IT-Grundschutzes sowie anderer Richtlinien und Vorgaben. Wenn die Vorgaben und Empfehlungen aus dem IT-Grundschutz umgesetzt werden, wird das Risiko eines erfolgreichen Angriffs deutlich verringert.

Das BSI stellt auf seiner Webseite weitere Informationen mit erforderlichen Präventivmaßnahmen und Hilfen im Schadensfall zur Verfügung:

https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen.html

Fortschrittliche Angriffe – Vorgehen der Angreifer