Trügerische Sicherheit: Aus diesen Gründen bleibt Ransomware weiterhin eine Gefahr

Sebastian Evers
Attingo Datenrettung Gmbh

Nach Emotet ist vor Emotet

Die Zerschlagung der Verbreitungswege und Netzwerke von Emotet, Anfang 2021, wird als Meilenstein in der Bekämpfung von Cyber-Kriminalität gefeiert. Fast jede größere Ransomware-Kampagne hatte Emotet dazu verwendet, um Netzwerke zu infiltrieren und Malware nachzuladen. Darunter waren diverse Unternehmen (Konzerne, KMUs), Behörden und staatliche Einrichtungen sowie Krankenhäuser. Emotet war auch bei dem Ransomware-Angriff auf den Heise Verlag sowie die Funke Mediengruppe ein Schlüsselelement für die Täter. Alleine in Deutschland soll sich der durch Emotet und Begleitschadsoftware verursachte Schaden auf etwa 14,5 Millionen Euro belaufen. [1]

Emotet galt lange Zeit als die weltweit gefährlichste Schadsoftware. In Anbetracht dieser Einstufung hat die Abschaltung der Netzwerke rund um Emotet sowie die durch die Ermittlungsbehörden initiierte Selbstdeinstallation der Malware den Cyber-Kriminellen einen schwerwiegenden Schlag versetzt. Die Bekämpfung und Beseitigung von Emotet ist nur eine gewonnene Schlacht unter unzähligen – in einem Krieg von ungeahntem Ausmaß. Es ist ein stetiges Wettrüsten, und die Methoden der Täter werden zunehmend perfider. Der Sieg über Emotet ist nur ein abgeschlagener Kopf der Hydra. Mit der Stilllegung des gefürchteten „Downloaders“ werden Ransomware-Angriffe nicht einfach aufhören. Das Geschäft mit „Malware-as-a-service“ boomt dennoch weiterhin. Es ist also nur eine Frage der Zeit, bevor ein „Emotet 2.0“ auf der Bildfläche erscheint – weitaus besser und effektiver als sein berüchtigter Vorgänger.

Doch auch ohne Emotet gibt es mehr als genug Angriffe und ein Ende ist leider nicht in Sicht. Begünstigt durch verschiedene Gründe zieht es mehr und mehr Kriminelle in den Sumpf der Ransomware-Erpressung.

Krypto-Währung begünstigt Ransomware-Erpressungen

„Follow the money“ lautet eine der kriminalistischen Faustregeln. Folgt man der Spur des Geldes, gelangt man auf diesem Weg früher oder später auch zu den Strippenziehern – so die grundlegende Idee. Allerdings sind die Täter bei Ransomware-Erpressung durch die schwierige – nahezu unmögliche – Nachverfolgung gezahlter Kryptowährungen quasi nicht ausfindig zu machen. Wo früher bei Erpressungen die Geldübergabe der größte Schwachpunkt des Verbrechens gewesen ist, ist dieses Risiko heute nahezu null. Auch pseudonyme Krypto-Währungen lassen sich über dezentrale Exchanges anonymisieren, von allen Anhaltspunkten kriminellen Ursprungs reinwaschen und in sauberes Geld umwandeln. Somit lässt sich der Wechsel von Krypto in Bargeld, ohne Hinweise auf kriminellen Ursprung, durchführen.

Erpresser agieren in der Regel global

Die Zuständigkeit der jeweiligen Ermittlungsbehörden endet an den Landesgrenzen. Das wissen auch die Täter. Man kann also davon ausgehen, dass die Ransomware-Erpresser stets länderübergreifend agieren. Oftmals werden die personellen Strukturen in Osteuropa und Asien vermutet. Durch entsprechende OPSEC Maßnahmen ist eine Identifizierung der Täter fast unmöglich. Mit der Koordination der Angriffe aus einem anderen Land – oder mehreren anderen Ländern – ist es für lokale Ermittlungsbehörden nicht möglich effektiv gegen Täter vorzugehen. Die Verständigung der Polizei ist in vielen Fällen nur ein Placebo. Der Umstand schreckt die Täter nicht ab, ihre Verbrechen zu begehen. Sie wissen, dass sie geschützt durch mehrere Landesgrenzen beinahe nichts zu befürchten haben. Denn es kommt nicht immer zu einer landesübergreifenden Zusammenarbeit von Ermittlungsbehörden, wie im Falle von Emotet.

Verbrechen auf Vertrauensbasis

Die Kriminellen haben sich den Ruf erarbeitet, dass sie die Daten nach Bezahlung der Lösegelder tatsächlich zur Verfügung stellen. Eine gewisse Romantisierung hat sich dadurch eingeschlichen. Es wird von einer „Ganovenehre“ gesprochen. Allerdings verfolgt die stringente Einhaltung der getroffenen Vereinbarungen gegenüber den Opfern ein klares Ziel: Es geht nur darum, die Zahlungsbereitschaft der Betroffenen nicht zu gefährden. Alles daran ist geschäftliches Kalkül. Es geht ausschließlich darum, dass die geforderten Lösegelder gezahlt werden. Solange jedem klar ist, dass die Erpresser die Daten gegen Zahlung freigeben, werden Betroffene auch dafür bezahlen, wenn ihnen keine Alternative zur Verfügung steht. Würden die Täter nach erfolgter Zahlung keine Daten herausgeben, würden sie sich damit zukünftige Geschäfte kaputt machen. Es ist eine Art perverser Symbiose zwischen Tätern und den Opfern entstanden.

Zahlungsbereitschaft ist ein Problem

In der Situation des Opfers erscheint der Ausweg meist alternativlos: Wenn die Angreifer die digitale Infrastruktur lahm gelegt haben, dann stellt die Zahlung des geforderten Lösegelds in den meisten Fällen die schnellste und effektivste Methode dar, um zeitnah wieder handlungsfähig zu sein. Stillstand kostet in jeder einzelnen Minute große Summen. Die Erpresser wissen das genauso gut wie ihre Opfer. Und das beständige Ticken der Uhr ist auf krimineller Seite, denn in den meisten Fällen zahlen die Betroffenen. Das Lösegeld ist in der Regel geringer als der finanzielle Aufwand, der erforderlich wäre, um alles von Grund auf neu aufzusetzen. Ganz zu schweigen vom durch den Stillstand bedingten Verlust. Einziger Ausweg bleibt die Datenrettung von etwaigen gelöschten aber nicht verschlüsselten Backup-Systemen.

Lösegeld-Versicherungen wecken Begehrlichkeiten

Vor Cyber-Angriffen ist niemand sicher, es wird im Laufe der Zeit jeden treffen – die Frage ist nur wann. Das haben die vergangenen Jahre immer wieder gezeigt. Viele Versicherungen bieten seit Längerem umfassenden Schutz gegen Hacker- und Cyber-Angriffe. Unternehmen schließen diese Versicherungen zunehmend mit immer höheren Abdeckungssummen ab, sodass die hohen Lösegeldforderungen übernommen sind, sollte man trotz allem einem Angriff durch Ransomware-Erpresser zum Opfer fallen. Doch diese vermeintliche Sicherheit ist ein großes Problem. Sie ist der Tropfen Blut im Piranha-Becken. Die Erpresser wissen über die hohen Abdeckungssummen Bescheid. Sie können sich sehr sicher sein, dass ein Angriff sich auch rentiert und dass das Opfer schnell bereitwillig zahlen wird, wenn eine Versicherung involviert ist. Sie können ebenso davon ausgehen, dass das Lösegeld in beliebiger Höhe angesetzt werden kann. Dieser Umstand führt dazu, dass sich immer mehr Kriminelle dazu berufen fühlen, mit Ransomware-Angriffen auf zahlungskräftige Klientel abzuzielen. Und wenn eine Versicherung wie Axa für Lösegelder künftig nicht mehr zahlt, wird sie selbst zum Ziel einer Attacke.

Schutz vor Ransomware-Angriffen, Vermeidungs-Strategien [2] Erster Schritt: Vorbereitung

Kontrolle ausüben: Updates und Patches aktuell halten

Da bekanntermaßen die Ausnutzung von Sicherheitslücken die Infektion mit Malware begünstigt, ist der erste Schritt zur Prävention von Ransomware-Angriffen eine aggressive Patch- und Update-Strategie zur Absicherung der potenziellen Zielsysteme. Dazu zählt auch die Vermeidung des Einsatzes von Hardware, über die man zu wenig eigene Kontrolle hat.

Besonders geschützte Sicherheitskopien

Sicherheitskopien und deren Schutz sind ebenfalls von sehr großer Bedeutung. Das hohe Risiko von Ransomware bei groß angelegten Cyber-Angriffen auf Firmen resultiert daraus, dass die Angreifer Backup-Dateien und Datensicherungssysteme zerstören und die tagtäglich genutzten Dateien und Systeme verschlüsselt werden. Im Hinblick auf diese Gefahr sollten entsprechende Dokumente, Datenbankensysteme etc. in eng getakteter Abfolge offline an Orte kopiert werden, die für die Eindringlinge schwer bis gar nicht zu erreichen sind (z.B. Tapes, externe Festplatten oder Offline-Storage-Backups). Dabei sollte auch überprüft und getestet werden, ob sich die Daten ohne großen Aufwand aus den Backups wiederherstellen lassen. Permanent verbundene Netzwerklaufwerke (NAS) und auch Cloud-Speicher sind nicht komplett sicher, denn das Risiko, dass verschlüsselte Dateien automatisch dorthin gesichert werden und dadurch bestehende Backups überschreiben, ist immens.

Vorfallreaktionspläne

Es sollten spezifische Vorfallsreaktionspläne (Incident-Response-Plan, auch: IRP) für Ransomware-Attacken entwickelt werden, um sich auf gezielte Angriffe mit Krypto-Trojanern vorzubereiten, welche große Teile von Unternehmen lahmlegen könnten. Der Reaktionsplan sollte detailliert beschreiben, welche Personen was zu tun haben, sobald der Verdacht einer Netzwerk-Infiltration oder einer Ransomware-Attacke vorliegt. Nur auf diese Weise ist eine schnelle Reaktion umsetzbar – gleichzeitig aber auch eine mahnende Bewusstseinbildung im Vorhinein möglich. Für die Abwehr von Ransomware ist jede Sekunde entscheidend, welche dem IT-Security-Team bleibt, um die Verschlüsselung durch Krypto-Programme zu unterbinden oder zu unterbrechen.

Umfassende Mitarbeiter-„Awareness“

Diesem Aspekt gebührt besonders hohe – wenn nicht die höchste – Priorität: Umfassende Sensibilisierungsmaßnahmen und Schulungen („Awareness“-Training) für die Anwender sind eine unumgängliche wie auch sehr effektive Schutzmaßnahme, um sich gegen potenzielle Angriffe zu wappnen. Dadurch wird das Risiko reduziert, dass Angestellte auf Phishing-Mails – insbesondere Spear-Phishing-Mails – hereinfallen und damit die Malware ins firmeninterne Netzwerk holen. Viele Cyber-Angriffe setzen dabei auf Social-Engineering-Taktiken. Die Mitarbeiter sollten sich der Gefahr bewusst sein und lernen, wie eine verdächtige Nachricht enttarnt werden kann, um einer Infektion entgegen wirken zu können.

Sicherheit durch „Security by Design“
So banal es vielleicht auch klingen mag, eine durchdachte Netzwerktopologie, bei der Anwender nur soweit Zugriffe haben als sie es für den Arbeitsalltag benötigen, hilft in vielen Fällen vor einer massenhaften Ausbreitung und weitreichenden Vernichtungen. Ebenso verringern sich die Einfallsverktoren wenn nicht zwingend benötige Dienste – beispielsweise von NAS und IoT – nicht direkt über offene Ports im Internet zur Verfügung stehen, sondern sich hinter dem Schutz einer VPN-Firewall verstecken können. Ausreichend starke Passwörter für Logins auf Samba-Shares oder Administrationskonten setzen wir in diesem Umfeld selbstredend voraus.

Zweiter Schritt: Entdecken und Feststellen

Organisationen können den potenziellen Schaden, welchen ein Angriff mit Ransomware verursachen könnte, minimieren, wenn die Malware früh genug entdeckt werden kann. Network-Intrusion-Detection-Systeme (NIDS) haben während der Infektions- und Exploitphase die Möglichkeit Signaturen sowie IOCs (Indicators of compromise) auszumachen. Mithilfe von Threat Intelligence hat IDS die Möglichkeit, um die Aktivität von Ransomware im Netzwerk aufzuspüren, zu stoppen oder zumindest eine Warnung an die IT-Sicherheitsbeauftragten zu senden.

Namhafte IDS-Anbieter haben zahlreiche Erkennungsmuster in ihre Systeme integriert, mit deren Hilfe Netzwerk-Anomalien aufgedeckt werden können. Diese Aktivitäts-Muster können sich je nach Ransomware und Ransomware-Version unterscheiden. Aus dem Grund ist es notwendig mehrere Verteidigungslinien aufzubauen. Trotzdem sind die Signaturen ein guter Ansatz, da somit die in den meisten Unternehmen eingesetzten Systeme zur Abwehr mit einbezogen werden.

Das Stoppen ausführbarer E-Mail-Anhänge
Generell sind alle Tools hilfreich, welche Attachments und Executables in Phishing-E-Mails ausfindig machen können, um Ransomware den Zugang zum Unternehmens-Netzwerk zu verwehren. Mit derartigen Schutzmaßnahmen existiert schon einmal eine grundlegende und automatisierte Verteidigung.

Überwachung temporärer Dateien sowie Anwendungsdaten
Mit der Tatsache, dass Ransomware zumeist aus den Verzeichnisordnern %appdata% oder %temp% startet, liefert einen weiteren Hebelpunkt: Die Überwachung dieser Ordner sowie darin ausgeführter Anwendungen und Programme ermöglicht es Ransomware zu entdecken, bevor diese die Gelegenheit hat Dateien zu verschlüsseln. Wie schon in der Exploit-Phase kann man über Netzwerk-Regeln die Ausführung sowie Verbreitung von Malware wie Ransomware visualisieren. Oder man transferiert seine Workstations auf Linux-Systeme, denn dort gibt es besagte Ordner in dieser Form erst gar nicht.

Vssadmin-Befehle beaufsichtigen
Angriffe auf Backups und der Versuch die Datensicherungen zu zerstören erlauben es, ebenfalls die Ransomware-Aktivitäten aufzudecken, bevor die Verschlüsselung gestartet werden kann. Die Ausführung von „vssadmin“-Kommandos sollte dabei besondere Beachtung finden und nach Möglichkeit mit einem Alarm verknüpft werden. So haben Verantwortliche eine reelle Chance, rechtzeitig einzugreifen und gefährdete Computer und Netzwerklaufwerke vor der Ransomware-Verschlüsselung zu schützen.

Kontrolle von Registry-Einträgen und Dateiendungen
Auch die Überwachung der Kommunikation des Command-and-Control Servers (C&C) ist eine Möglichkeit, um anhand von Netzwerk-Signaturen, der Vergabe von Dateinamen und Änderungen in der Registry zu erkennen, dass beispielsweise der zu Beginn der Verschlüsselungsphase erforderliche Schlüsselaustausch erfolgt. Die Ransomware Locky fiel dadurch auf, dass immer mehr Dateien mit der Dateierweiterung .locky auftauchten. So konnte der Befall mit dem Krypto-Trojaner bemerkt werden.

Leider benutzen viele Krypto-Trojaner mittlerweile einzigartige Dateierweiterungen, die von Befall zu Befall unterschiedlich sind. Zudem ist die Umbenennung der verschlüsselten Dateien durch die Ransomware in der Regel ein recht später Schritt, der ziemlich zum Ende des Krypto-Angriffs erfolgt. Dennoch können die Indikatoren bereits ausreichen, um das Ausmaß des Angriffs eingrenzen zu können – wenn der Angriff schon nicht verhindert werden kann.

Dritter Schritt: Eindämmung und Quarantäne

Ist bereits ein Gerät der Ransomware zum Opfer gefallen, so gibt es nach wie vor die Möglichkeit den Angriff auf dieses Umfeld zu beschränken, um den Angriff auf Dateien im Netzwerk zu verhindern.

Endpoint-Security-Systeme, die ausführbare Dateien erkennen und die Prozesse stoppen können, sind ein guter Ansatz für eine Eingrenzung von Ransomware-Attacken. Wird schadhafte Malware entdeckt, so wird die Netzwerk-Verbindung unmittelbar getrennt und die Schadsoftware ist auf dem jeweiligen System isoliert, sodass sie keine Dateien im Netzwerk verschlüsseln kann.

Vierter Schritt: Systembereinigung und Entfernung von Ransomware / Malware

Ist der Ransomware-Angriff identifiziert und eingedämmt worden, ist es unabdingbar, die Malware sowie etwaige Spuren zu entfernen. Es empfiehlt sich betroffene Systeme zu ersetzten, anstatt diese nur zu „säubern", da sich diverse Malware überaus gut in den Tiefen der Hardware zu verstecken weiß. Möglicherweise wurden bereits Router oder Drucker infiziert, in dem sich die Dateien verstecken, um für den Fall einer Entdeckung vor einer effektiven Bereinigung sicher zu sein und im Anschluss das Netzwerk erneut zu infizieren.

Wann immer man sich für eine Säuberungsaktion entschließt, anstatt für das Ersetzen kompletter Hardware, sollte im Nachhinein eine penible Überwachung auf IOC und Signaturen erfolgen, um ein wiederholtes Aufkommen der Ransomware-Infektion schnellstmöglich zu unterbinden.

Fünfter Schritt: Wiederherstellung von Netzwerken, Systemen und Daten

Die Wiederherstellung umfasst zunächst einmal das Wiedereinspielen von Datensicherungen und Backups der zerstörten und verschlüsselten Dateien. Für ein Unternehmen, das auf umfassende und geprüfte Sicherheitskopien zurückgreifen kann, kann ein Krypto-Angriff mit Ransomware nahezu folgenlos bleiben. Es ersetzt die befallenen Geräte oder säubert sie und rekonstruiert den Datenbestand aus den Backups – ratsamerweise aber zumindest auf neuen Datenträgern, um die infizierten Originale für spätere Ermittlungstätigkeiten oder noch benötigte Datenwiederherstellungen zur Verfügung stehen. Dabei wird man eine kurzzeitige Unterbrechung bei den IT-Anwendungen in Kauf nehmen müssen. Es ist recht unwahrscheinlich, dass die Attacke unter derartigen Voraussetzungen zu einem tagelangen Problemzustand wird – auch wenn es in dieser Hinsicht bereits Fälle gegeben hat, bei denen z.B. NotPetya einen internationalen Logistikkonzern beinahe vollständig lahm gelegt hat. Zehn Tage lang arbeitete das Unternehmen vollkommen analog, bis die IT-Infrastruktur wieder online war.

Wie kam es zu dem Ransomware-Befall?

Bei jedem Cyber-Angriff lohnt sich eine genauere Beleuchtung, wie die Infektion stattgefunden hat. Waren es Phishing-E-Mails oder web-basierte Angriffs-Kits? Wenn es ein web-basierter Angriff gewesen ist, wie wurde der verantwortliche Anwender auf die Internetseite gelockt? Wenn man herausfinden kann, wie Ransomware in die Systeme und ins Netzwerk gelangen konnte, dann lassen sich mit diesen Erkenntnissen Abwehr- und Erkennungsmethoden maßgeblich optimieren und Schwachstellen für die Zukunft minimieren.

Die Bedrohung durch Ransomware wird nicht verschwinden

Ransomware-Angriffe gegen KMUs, Konzerne, Behörden und öffentliche Einrichtungen sowie Krankenhäuser stellen eine Gefahr dar, welche trotz ihrer Häufigkeit erst die Spitze des Eisbergs des potenziell Möglichen bildet. Aufgrund der Attraktivität solcher Angriffe und der damit erzielten Erfolge werden Täter zunehmend häufiger darauf setzen. Und die Angriffe werden sukzessive an Schlagkräftigkeit und Gefährlichkeit dazu gewinnen, sodass noch gewaltigere Schäden, mit noch höheren Kosten die Folge sein werden.

Die Wenigsten sind auf Datenverlust durch derartige Ransomware-Angriffe vorbereitet – egal, ob groß oder klein. Die kaum absehbaren Folgen stellen einen weitaus kritischeren Verlust dar, als die Bezahlung der geforderten Lösegeldsumme: Imageverlust, Produktivitätseinbußen, eingeschränkte Geschäftsfähigkeit, beeinträchtigte Kundeninteraktion, Datendiebstahl oder die Veröffentlichung brisanter Daten. Die erfolgreiche Abwehr eines Ransomware-Angriffs hängt davon ab, wie gut man darauf vorbereitet ist, die Indizien für das Treiben von Krypto-Trojanern oder anderer Malware zu erkennen und verdächtige Aktivitäten zeitnahe zu stoppen.

Besser auf Ransomware vorbereitet sein

Es ist stets besser, auf den Extremfall vorbereitet zu sein, der niemals eintritt – und das wird er mit an Sicherheit grenzender Wahrscheinlichkeit dennoch irgendwann -, anstatt beim Eintreten des Extremfalls schutzlos ausgeliefert zu sein. Mit einfacheren Worten: Vorsicht ist besser als Nachsicht.

Quellen: **[1]** https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html **[2]** https://www.attingo.de/blog/so-schuetzen-sie-sich-effektiv-gegen-ransomware-angriffe/

Sebastian Evers

Sebastian Evers ist seit 2010 als Kundenbetreuer bei der für ganz Deutschland zuständigen Attingo Datenrettung GmbH in Hamburg tätig. Regelmäßig bloggt er zu spezifischen Themenfeldern aus dem Bereich der professionellen Datenrettung und informiert über die „Dos and Dont's".

Foto: Privat