Umfassender Schutz vor Cyberangriffen und Ransomware

Controlware Cyber Defense Center – Incident Response as a Service

Es gibt Tatsachen, vor denen Sicherheitsverantwortliche und Entscheider in Unternehmen nicht die Augen verschließen sollten. Die Entwicklungen der letzten Monate bestätigen es: Der kontinuierliche Incident-Response-Fall wird zum „Daily Business" und ist schon längst nicht mehr die seltene Ausnahme. IT-Sicherheitsvorfälle passieren – und zwar immer öfter.

Die meisten Unternehmen und Organisationen sind jedoch nach wie vor nicht ausreichend auf einen Sicherheitsvorfall vorbereitet. Die Gründe hierfür liegen zum Beispiel im mangelnden Verständnis aktueller Angriffsmethoden, in fehlenden Budgets, fehlender Transparenz über Software-Schwachstellen, eingeschränkter Detektionsfähigkeit unbekannter Bedrohungen und Anomalien oder weil Erkenntnisse über Vorfälle nicht entsprechend kommuniziert werden.

Während die einen Unternehmen glauben, zu unbedeutend zu sein, um für Angreifer ein attraktives Ziel abzugeben, überschätzen andere bis heute die Wirksamkeit ihrer Sicherheitsstrategie und überprüfen diese viel zu selten. Mit schwerwiegenden Konsequenzen: In diesen Fällen geraten Unternehmen in der Abwehr neuer Bedrohungen schnell ins Hintertreffen – notwendige Investitionen in Sicherheitstechnologie und Experten-Know-how unterbleiben.

Controlware stellt mit seinen Managed Cyber Defense Services Ressourcen bereit, an denen es Unternehmen oft mangelt, um ihre Assets kontinuierlich zu schützen. Basierend auf Sensorkomponenten und umfassender Analyse-Infrastruktur führender Hersteller werden Malware-Infektionen und Infektionsversuche frühzeitig detektiert, die darauf ausgelegt sind, unerkannt durch die klassischen Perimeter-Sicherheitssysteme wie Firewall, Proxy, Anti Virus, IDS/IPS etc. zu gelangen. Je komplexer eine Infektionskette ist, desto wichtiger ist es, diese so früh wie möglich zu erkennen.

Zusätzlich zum Einsatz einer geeigneten Advanced Malware Protection-Lösung ist es vor allem wichtig, den Kontext eines Angriffs zu verstehen, um darauf angemessen reagieren zu können. Für die Qualifizierung eines Sicherheitsvorfalls hat der Kunde Zugriff auf das Experten-Know-how der Analysten im Controlware Cyber Defense Center (CDC). Neben der Qualifizierung eines Angriffs begleiten diese das IT-Team des Kunden bei der Umsetzung geeigneter Abwehrmaßnahmen sowie bei der Entwicklung einer nachhaltigen Abwehrstrategie, um ähnliche Vorfälle in Zukunft zu vermeiden.

Insbesondere der deutsche Mittelstand als „das Rückgrat der deutschen Wirtschaft" ist heute verwundbar wie nie: Mit über 60 Prozent sind mittelständische Unternehmen laut Bitkom überproportional häufig von Cyber-Attacken betroffen. Aufgrund ihres besonders schützenswerten geistigen Eigentums sind sie für Cyber-Angreifer ähnlich attraktiv wie Großunternehmen und ebenfalls einer hohen Bedrohungslage ausgesetzt. Mittlerweile muss jedes Unternehmen damit rechnen, zum Ziel von Attacken zu werden – unabhängig von seiner Größe.

Ein häufiger Angriffsvektor sieht folgendermaßen aus: Am Anfang steht oftmals eine „Malspam"-E-Mail (z.B. in Form von Fake Telekom/Vodafone-Rechnung, Google Docs/Dropbox Link, DHL Tracking etc.), die einen Malware-Dropper (mit oder

ohne Benutzerinteraktion) im Anhang verbirgt oder einen Link enthält. Wird der Anhang geöffnet, lädt der Dropper (in Office-Dokumenten beispielsweise via Macro) die eigentliche Malware nach und startet diese. Danach werden gegebenenfalls Hintertüren eingerichtet und die Malware auf dem System persistiert. Beim Öffnen eines Links wird entweder ein Dropper heruntergeladen oder der Benutzer öffnet eine Seite, die ihn nach einem Fingerprinting des von ihm eingesetzten Betriebssystems, Browsers und aktivierter Plugins auf eine Exploit-Kit-Seite weiterleitet, die einen für ihn „passenden" Exploit ausliefert. Nach erfolgreicher Detonation des Exploits ist das System infiziert und unter der Kontrolle des Angreifers. Ein mögliches Ziel kann unter anderem darin bestehen, Zugangsdaten zu entwenden und Tastatureingaben zu überwachen. In der Regel suchen Angreifer dann nach weiteren Sicherheitslücken im Netzwerk, um an immer wertvollere Informationen und Assets zu gelangen. Auch aktuelle Ransomware-Kampagnen folgen diesem Muster.

Folgender aktuell bei einem unserer Kunden aufgetretener Incident verdeutlicht die Notwendigkeit, neben kontinuierlicher Überwachung durch entsprechende Sensorik die richtigen Abwehrmaßnahmen zu empfehlen und einzuleiten, da vor allem der Faktor Zeit eine wichtige Rolle spielt. Ein Sensor-System des Kunden meldete ein maliziöses E-Mail-Attachment und nahm dieses nach automatisierter Sandbox-Analyse in Quarantäne. Dadurch wurde im Controlware CDC parallel ein Incident eröffnet, welcher um die in der Sandbox-Analyse ermittelten Indikatoren automatisch angereichert wurde. Wenige Minuten später konnte dieses Attachment seitens Controlware bereits einer aktiven Malspam-Kampagne zugeordnet werden, durch die gerade massiv die Verteilung von Jaff Ransomware erfolgte. Die verwendeten Malware-Dropper wurden in diesem Fall in ein PDF eingebettet. Der User sollte durch entsprechende Informationen zum Öffnen des Word-Dokuments sowie zum Aktivieren von Makros verleitet werden, um die eigentliche Malware (in diesem Fall Jaff Ransomware) nachzuladen und auszuführen.

Durch die vorhandenen Threat Intelligence-Informationen im Controlware CDC, die bereits zu dieser Kampagne sowie Malware existierten, war es möglich, dem Kunden binnen kürzester Zeit Abwehrmaßnahmen zu empfehlen, die er auf seine existierenden Sicherheitssysteme ausrollen konnte.

Traffic

- **Alle bereits zu dieser Kampagne bekannten URLs (in diesem Fall 17), von denen die Dropper versuchten, die Malware nachzuladen, konnten proaktiv auf dem Proxy gesperrt werden.**
- **Alle Command & Control Domains wurden zusätzlich in das DNS-Sinkhole hinzugefügt, um Anfragen zu diesen Domains „ins Leere" laufen zu lassen.**

Malware

- **Alle bekannten File-Hashes zu den verwendeten Droppern sowie der Ransomware konnten als Application Control („Blacklist")-Einträge auf die Endpoints des Unternehmens verteilt werden, um deren Ausführung proaktiv zu verhindern.**

Die Abwehrmaßnahmen für diesen Incident verhinderten durch diese Kampagne proaktiv weitere mögliche Infektionen auf anderen Infektionsvektoren. So werden Malware Dropper nicht immer als Anhang einer E-Mail verschickt, die sich inline im MTA-Modus blockieren lassen, sondern zum Teil auch als Download-Link. Weiterhin ist es beispielsweise möglich, dass ein User auf seinem Firmenrechner eine solche E-Mail aus seinem privaten Webmailer heraus öffnet.

Eine Infektionskette lässt sich nicht immer so früh stoppen, wie in diesem Beispiel. Vor allem im Bereich Web-Browser (Skripte, Downloads unbekannter Objekte, dateilose Infektionen durch Exploits) ist es möglich, dass ein Infektionsversuch bzw. eine Infektion erst zeitverzögert erkannt wird. Dies kann unter anderem an der Analyse-Dauer in der Sandbox liegen oder weil bereits eine Bestandsinfektion vorliegt und man erst spätere Phasen detektiert (zum Beispiel Command & Control-Kommunikation). In diesen Fällen ist es wichtig, zu verifizieren, ob ein Infektionsversuch, zum Beispiel durch einen Exploit, erfolgreich war. Auf Basis der Informationen, die von den Sensor-Systemen gemeldet werden, angereichert mit den eigenen Analyse-Ergebnissen der Analysten des Controlware Cyber Defense Centers, erfolgt die Suche nach Indikatoren der Infektion auf dem betroffenen System, um die entsprechenden Abwehrmaßnahmen einzuleiten. Auch eine weitere Ausbreitung im Netzwerk wird unter Nutzung weiterer Datenquellen und Logs verifiziert.

Wer Cyber-Kriminellen nicht völlig freie Hand lassen möchte, sollte seine aktuelle Sicherheitsstrategie regelmäßig überprüfen und ergänzende Maßnahmen treffen. Das kann den Einsatz sensorbasierter Detektionslösungen und die Einführung solider Incident-Response-Strukturen beinhalten und so einen möglichen Schaden bereits im Keim ersticken. Wichtig ist, entsprechendes Know-how im Hause zu haben – also Experten, die in der Lage sind, Sicherheitsvorfälle in ihrer Kritikalität richtig zu bewerten und geeignete Abwehrmaßnahmen zu empfehlen. Ist das nicht der Fall, sind Managed Security Services wie die Controlware Managed Cyber Defense Services eine gute Alternative, die gleichzeitig auch ökonomisch attraktiv sind.

Frank Melber,
Head of Cyber Security Services,
Controlware GmbH

Benjamin Heyder,
Senior Security Architect,
Controlware GmbH