Großes Software-Update für iSecurity Anti-Ransomware

Cyber-Attacken können jetzt simuliert werden

Rödental, 17. Mai 2020 - Raz-Lee Security kündigt ein umfangreiches Upgrade für iSecurity Anti-Ransomware (ATP) an - der weltweit einzigartigen und jetzt umfassend erweiterten Lösung zum Schutz von IBM i IFS-Dateien gegen Ransomware und andere Arten von Malware, die IBM i IFS-Dateien beschädigen können.

Die Lösung wurde um einen Angriffssimulator erweitert, der absolut sicher zu verwenden ist, da er nur in einem isolierten bekannten Ordner auf IBM i funktioniert. Er ist in der Lage, einen „typischen" Angriff zu simulieren wie er in der Realität häufig vorkommt. Der Simulator kann so eingestellt werden, dass er Angriffe bekannter Ransomware wie WannaCry, CryptoLocker oder Jigsaw vortäuscht. ATP ist ebenfalls in der Lage, neue Verschlüsselungsmethoden aufgrund seiner Algorithmen zu entdecken und zu blockieren. Da Ransomware jetzt auch als Dienst im Darknet angeboten wird, wird regelmäßig eine Zero-Day-Ransomware (unbekannt) angezeigt. Die neue Funktion kann diese auch simulieren.

Es gab auch Ransomware-Angriffe auf die IBM i, darunter einige, die im Internet veröffentlicht wurden. Unter ihnen waren CryptoLocker, der 250.000 IFS-Dateien beschädigte und ein weiterer, der 500.000 IFS-Dateien verschlüsselte. Im letzten Fall wurde das geschädigte Unternehmen zur Zahlung von 200.000 US-Dollar aufgefordert, um den Entschlüsselungskey zu „kaufen". Wichtig zu wissen: Nur in 25% aller Fälle erhält der Geschädigte bei Ransomware-Attacken nach der Zahlung einen funktionierenden Entschlüsselungscode. Mit iSecurity Anti-Ransomware werden möglicherweise 1 oder 2 Dateien kompromittiert, das IFS ist aber in Gänze geschützt!

Ransomware-Attacken gehen von einem PC aus

Ransomware wird auf einem PC ausgeführt und greift jede Datei an, auf die sie Zugriff hat, auch auf freigegebene Dateien von Remote-Systemen. Einige Unternehmen mit IBM i-Installationen fühlen sich sicher, da keinen Internetzugang zulassen. Ransomware braucht keinen Internetzugang – bereits das Öffnen einer einfachen E-Mail genügt, um ein großes Unternehmen faktisch zu zerstören. Viele Verantwortliche wiegen sich in Sicherheit. Sie gehen davon aus, dass eine gute Antiviren-Lösung auf ihrer IBM i sie schützt. Ransomware gelangt jedoch nicht in die IBM i sondern startet von einem angeschlossenen PC aus. Zwar können die Ergebnisse einer Attacke durch Ransomware-Erweiterungen einer Antiviren-Software erkannt werden, es ist jedoch bereits viel zu spät.

Erkennen, unterbrechen, vom Netz trennen, Warnungen ausgeben

Die Anti-Ransomware verwendet mehrere Erkennungsmethoden gleichzeitig, um den Schaden zu minimieren, der an IBM-i-Dateien verursacht werden kann. Sie unterbricht den Angriff nach kurzer Zeit, trennt das IBM-i-System vom Netzwerk, sendet Echtzeitwarnungen an das übergeordnete SIEM-System und stoppt die Zugriffe, die vom infizierten Computer ausgehen. Es kann sogar vor Zero-Day-Angriffen schützen. iSecurity Anti-Ransomware bietet eine proaktive Lösung, während Antivirenlösungen reaktiv sind. Sie erkennen lediglich den durch einen Angriff verursachten Schaden, können ihn jedoch nicht stoppen.

Rasante Zunahme von Cyber-Attacken während der Corona-Krise

Während der Corona-Krise schließen Schulen, Unternehmen und ganze Gemeinden, um die Ausbreitung der Pandemie zu verlangsamen. Cyberkriminelle nutzen diese Krise aktiv für ihren eigenen finanziellen Gewinn. Google berichtet, dass zwischen dem 6. und 13. April täglich mehr als 18 Millionen Malware- und Phishing-E-Mails im Zusammenhang mit Covid-19-Betrug sowie mehr als 240 Millionen tägliche Spam-Nachrichten im Zusammenhang mit dem Corona-Virus angezeigt wurden. Laut den Bedrohungsforschern von VMware Carbon Black stiegen die Ransomware-Angriffe im März 2020 gegenüber Februar 2020 um 148% gegenüber dem Ausgangswert an. Attacken mit Erpressungs-Software machen 52% aller Angriffe aus - eine beispiellose Zunahme für VMware Carbon Black.

Verstärkte Forschung und Entwicklung bei Anti-Ransomware und Antiviren-Software

„Unsere Forschungs- und Entwicklungsabteilung hat sich auf die Verbesserung unserer ATP-Lösung konzentriert, um Unternehmen vor den Aktivitäten von Cyberkriminellen

abzusichern. Gerade in der globalen Krise ist es wichtig, jene zu stoppen, die sie ausnutzen wollen und die IT-Systeme von Unternehmen zu schützen“, sagt Robert Engel, Geschäftsführer von Raz-Lee in Deutschland.

Auch andere iSecurity-Lösungen erhielten Updates. So wurden iSecurity Anti-Virus, ICAP Client für iSecurity Anti-Virus und Native Object Integrity verbessert. iSecurity Anti-Virus bietet jetzt Funktionen zur Verarbeitung mehrerer Kanäle. Es ist möglich, die Scanlast auf acht parallele Kanäle zu verteilen und so die Wartezeit auf den Scan eines Objekts effektiv zu verkürzen. Mit dem ICAP Client für iSecurity Anti-Virus können Unternehmen den ressourcenintensiven Antiviren-Scanauftrag von IBM i auf einen schnelleren Dedicated Server laden. Dies ist besonders wichtig bei großen Installationen, sodass die IBM i weiterhin wichtige Aufgaben ausführen kann.

Unser Beitrag für Ihr Unternehmen

In Zeiten der Corona-Krise unterstützen wir Ihr Unternehmen dabei, Mitarbeiter und deren Familien zu schützen, gleichzeitig aber den Geschäftsbetrieb Ihres Unternehmens sicher fortzusetzen.

Wir bieten unseren neuen und bestehenden Kunden bis Ende 2020 kostenlosen Schutz mit iSecurity ATP mit einer Abonnementgebühr danach. Das neue iSecurity ATP ist sofort verfügbar und wird von Raz-Lee via kostengünstigem Remote Support implementiert.

Über Raz-Lee Security GmbH und iSecurity

Raz-Lee Security ist führender internationaler Anbieter von Sicherheits-, Auditing-und Compliance (SOX, PCI, HIPAA, etc.) Lösungen für die IBM i. Zu Raz-Lee-Kunden zählen Unternehmen aller Größen, von KMUs bis zu Unternehmen mit Hunderten von Systemen, in allen vertikalen Märkten und Branchen. Finanzinstitute wie Banken und Versicherungen sind besonders zahlreich unter der Raz-Lee Klientel vertreten.