Wenn MSPs zum Instrument der Cyberkriminellen werden: Angreifer nutzen Managed Services für Ransomware-Attacken auf deren Kunden

Chester Wisniewski, Principal Researcher bei Sophos, hat ein Gespür für Trends, und zwar welche neuen perfiden Methoden sich im kriminellen Online-Ökosystem entwickeln. Angriffe über Managed Service Provider (MSP) hat er kommen sehen. Die jüngsten Beispiele von attackierten Zahnarztpraxen bestätigen nun seinen Spürsinn. Allerdings können wenige Sicherheitsmaßnahmen bereits große Wirkung im Kampf gegen die Hacker erzielen.

Ransomware ist eine starke Waffe der Cyberkriminellen. Und es entwickelt sich ein neuer Trend – die Infizierung von Unternehmen über deren Managed Service Provider. Die jüngsten Opfer allein in den USA: Hunderte von Zahnarztpraxen und Kommunen. Chet Wisniewski, der Forensik und das Vorhersagen von cyberkriminellen Entwicklungen zu seinem Beruf gemacht hat, hatte die Probleme und Gefahren von MSPs bereits seit langem im Auge und empfiehlt konkrete Schritte zur Vermeidung.

Im Visier: Managed Service Provider
Angriffe auf ganze Lieferketten sind keine neue Erfindung. Sie kommen immer häufiger vor und erlangen zu Recht immer auch immer stärkere Aufmerksamkeit. Während es zahlreiche Methoden von Attacken über ganze Lieferketten gibt, ist dieser spezielle Typus – einen Service Provider zu kompromittieren, um Zugang zu seinen Kunden zu erhalten – stetig beliebter bei geschickten Ransomware-Kriminellen. Vor ein paar Jahren fielen einige Vorfälle ähnlicher Spielart auf. Die Zielscheiben waren Point-of-Sale (Pos) Service Provider. Damals lag die Absicht nicht im Infizieren mit Ransomware, sondern im groß angelegten Diebstahl von Kreditkarten. Diese Idee wurde nun weiterentwickelt, um gezielt Angriffe über den MSP auf bestimmte Gruppen oder Märkte zu fahren.

Ausblick: MSP-Attacken werden zunehmen
Für viele kleine und mittelgroße Unternehmen ist die Organisation ihrer IT ohne die nötigen Ressourcen eine schwierige Aufgabe. Warum diese also nicht bei einem Service Anbieter auslagern? Klingt nach einer klugen wirtschaftlichen Entscheidung und ist es in vielen Fällen auch. Die Managed Service-Industrie wächst sehr schnell, insbesondere bei Unternehmen, die damit kämpfen, diejenigen Technologien zu verwalten, die für einen modernen Betrieb heutzutage notwendig sind.

Dies bietet ein lukratives Potenzial für Angreifer und derartige Attacken auf MSPs werden zunehmen. Für MSPs bedeutet das, sich aktiv mit ihrer Sicherheit auseinanderzusetzen, unabhängig davon, welche spezialisierten Services sie anbieten. In den SophosLabs wurden bereits Kriminelle gesichtet, die Schwachstellen in den populären Kaseya und Bomgar Remote Management Plattformen ausnutzten, um sich Zugang zu deren Systemen zu verschaffen und sie dafür zu missbrauchen, Schadsoftware bei deren Kunden einzuschleusen.

Allerdings heißt es für MPSs jetzt nicht, den Kopf in den Sand zu stecken. Es gilt, dieses Problem systematisch im Keim zu ersticken. Folgende Schutzmaßnahmen können dazu beitragen:

1. Die verbindliche und durchgängige Einführung der Multifaktor-Authentifizierung für Mitarbeiter mit administrativen Rechten über Hunderte von Kunden-Netzwerken.
2. Keine gemeinsamen Anmeldeinformationen für Zugang zu Kunden-Netzwerken.
3. Es ist notwendig, den Fernzugriff sicherer zu machen. Idealerweise geschützt via VPNs. VNC und RDP sollten nicht mehr verwendet werden.
4. Instrumente zur Fernwartung wie Kaseya und Bomgar müssen zwingend aktuell gehalten werden, insbesondere im Zusammenhang mit den Sicherheitshinweisen der Vergangenheit.

Lichtblick: der Kreis dieser Kriminellen ist (noch) klein

„Gegenüber vielen anderen Sicherheitsproblemen und deren massiver Verbreitung in Kombination mit schwieriger Fehlerbehebung hat das Risiko für MSPs und deren Kunden einen entscheidenden Vorteil: der Kreis der Kriminellen ist noch überschaubar. Damit besteht die seltene Chance, mit geeigneten Schutzmaßnahmen eine größere Verbreitung zu verhindern und den Cyberkriminellen einen Schritt voraus zu sein“, resümiert Michael Gutsch, Channel Account Executive Managed Service Provider EMEA.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
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