Schmunzeln erlaubt: 5 schusselige Ransomware-Pannen

Skrupellos, organisiert, vernetzt: Ransomware ist längst kein Gelegenheitszeitvertreib gelangweilter Hacker:innen mehr, sondern ein kriminelles Geschäft mit hohen Um- und Einsätzen. Aber auch Cyberkriminelle sind am Ende nur Menschen, denen selbst perfekt geplante Ransomware-Angriffe mal missraten. Sophos nennt ein paar Pannen zum Schmunzeln und wie man gegen Ransomware vorsorgen kann.

Eine typische Ransomware ist eine ausgefeilte, menschen-geführte Attacke, bei der die Eindringlinge oft mehrere Tage bis zu Wochen im Netzwerk verbleiben, bevor sie ihre Erpressungen starten. Während dieser Zeit bewegen sie sich durch das Netzwerk, stehlen Daten, installieren neue Tools, löschen Backups und noch vieles mehr.

Zu jedem Zeitpunkt könnte der Angriff dabei entdeckt und blockiert werden, und das stresst besonders die Cyberkriminellen, die via Tastatur die Attacke kontrollieren. Sie müssen Taktiken mitten im Einsatz ändern, oder für die geplante Malware-Einsätze einen zweiten Anlauf nehmen, wenn der erste scheitert. Dieser Druck kann zu Fehlern führen. Auch Cybergangster sind schlussendlich nur Menschen.

Das Sophos Rapid Response Team hat während seiner Analysen in der letzten Zeit mehrfach über verpatzte Ransomware-Attacken geschmunzelt. **Hier die Top 5 der Ransomware-Pannen:**

1. Die **Avaddon**-Gruppe, die von ihrem Opfer gebeten wurde, doch die eigenen Daten zu veröffentlichen – man könne einen Teil nicht wiederherstellen. Die Gruppe, zu dusselig zu verstehen, was ihr Opfer im Sinn hatte, machte die Ankündigung, Opferdaten zu veröffentlichen, wahr und das betroffene Unternehmen kam so wieder in den Besitz der Daten.
2. Die **Maze**-Angreifer:innen, die eine große Menge Daten von einem Unternehmen stahlen,, nur um dann herauszufinden, dass diese unlesbar waren: bereits verschlüsselt von der DoppelPaymer Ransomware. Eine Woche vorher.
3. Die **Conti**-Spezialist:innen die ihre eigene, neu installierte Hintertür verschlüsselten. Sie hatten AnyDesk auf einem infizierten Rechner installiert, um sich Fernzugang zu sichern und rollten dann die Ransomware aus, die alles auf dem Gerät verschlüsselte. Natürlich auch AnyDesk.
4. Die **Mount-Locker**-Bande, die nicht verstehen konnte, warum ein Opfer sich weigerte zu zahlen, nachdem sie eine Stichprobe geleakt hatten. Warum auch? Die veröffentlichen Daten gehörten zu einer ganz anderen Firma.
5. Die Angreifer:innen, die die Konfigurations-Dateien für den FTP Server, den sie zur Datenexfiltration nutzten, zurückließen. Damit konnte sich das Opfer einloggen und die gestohlenen Daten sämtlich löschen.

„Die gegnerischen Pannen, die uns ins Auge fielen, sind ein Beweis dafür, wie überfüllt und kommerzialisiert die Ransomware-Landschaft mittlerweile ist“, sagt Peter Mackenzie, Manager des Sophos Rapid Response Teams. „Als Ergebnis dieses Trends findet man verschiedene Angreifer:innen, die das gleiche potenzielle Opfer anvisieren. Rechnet man den Druck, der von Sicherheitssoftware und Incident Respondern ausgeht, dazu, ist es verständlich, dass die Attacken fehleranfällig werden.“

Neu: Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
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