Ransomware: Lassen Sie sich nicht erpressen

Die Geiselnahme von Daten, die sich auf privaten Computern oder Firmenservern befinden, ist bei Cyberkriminellen beliebt und für die Geschädigten eine Katastrophe. Vielen scheint das Begleichen der Forderungen die einzige Alternative zum Datenverlust. Ein Irrtum.

Von Chester Wisniewski, Senior Security Advisor, Sophos

Die Strafverfolgungsbehörden melden seit einigen Jahren einen rasanten Anstieg von Ransomware. War diese Form der Malware zunächst für die Erpressung von Endverbrauchern konzipiert so erweiterten Cyberkriminelle aufgrund des anhaltenden Erfolgs den Radius ihrer Angriffe bald auch auf Serverumgebungen. Die Malware verschafft sich Zugriffsrechte zu den Daten auf einem Computer und verschlüsselt sie. Damit sind alle Informationen zwar noch auf der Festplatte vorhanden, allerdings für den Besitzer völlig unbrauchbar. Um sie wieder nutzen zu können, muss ein Schlüssel erworben werden, den Preis bestimmen die Angreifer. Eines der wohl bekanntesten Opfer ist die Polizei in Tennessee, aber auch andere öffentliche Einrichtungen und Unternehmen wurden schon Opfer von Datenkidnappern.

Ist das Zahlen von Lösegeld ratsam?
Um auf die Forderung von Lösegeld richtig zu reagieren, müssen die Geschädigten einen kühlen Kopf behalten und sich darüber klar werden, mit welcher Form von Ransomware sie es zu tun haben:

Lockscreen-Ransomware öffnet ein Fenster auf dem Bildschirm und übernimmt den Computer oder das Mobilgerät. Häufig wird diesen Angriffen das Mäntelchen der Justiz übergezogen, indem der Betroffene eines Verbrechens oder illegalen Zugriffs über seinen Rechner bezichtigt wird. Gleichzeitig erfolgt das Angebot, die Sperrung gegen Zahlung einer Gebühr wieder aufzuheben.

Verschlüsselungs-Ransomware lässt zwar weiterhin den Zugriff auf Programme zu, verschlüsselt aber sämtliche Dateien auf dem Rechner, sodass der Eigentümer diese nicht mehr öffnen kann. Gewöhnlich poppt nach eine Weile ein Fenster auf, dass den Entschlüsselungscode anbietet – und den Preis hierfür nennt.

Lockscreen-Ransomware hat den Vorteil, dass die Sperre in den meisten Fällen mit ein wenig technischem Wissen umgangen werden und man sich das Zahlen eines „Lösegelds“ sparen kann. Anders sieht es bei Verschlüsselungsattacken aus. Aktuelle Versionen wie CryptoLocker, CryptoWall oder TeslaCrypt lassen solche Umgehungstaktiken nicht zu. Falls also kein Backup besteht, stehen die Geschädigten ohne den Dechiffrierungsschlüssel also tatsächlich vor dem Rechner wie der Ochs vorm Berg.

Grund dafür ist die sogenannten Public Key Cryptography, die zum Verschlüsseln und Entschlüsseln verschiedene Codes benutzt. Die Cybergangster generieren zwei Schlüssel und senden lediglich einen an die Ransomware auf dem befallenen Rechner, um die Verschlüsselung durchzuführen. Allerdings hilft es nun nichts, diesen auf dem Rechner befindlichen Code aufzutreiben, da er nicht dabei helfen kann, die Verschlüsselung aufzuheben. Der zweite Code ist im Besitz der Kriminellen.

Zahlen oder nicht?
Die übliche Lösegeldpreisspanne liegt bei rund 100 bis 300 Euro. Es ist zu beobachten, dass der Rechner in den meisten Fällen nach erfolgter Zahlung tatsächlich wieder freigegeben wird. Mit einem Ehrenkodex wie diesem stellen Ganoven sicher, dass die Zahlungsmoral der Opfer nicht einbricht.

Experten raten: Nein!
Dem steht der Rat vieler Experten entgegen, einer Erpressung nicht zu folgen und auf keinen Fall zu zahlen. Das ist leichter gesagt als getan, solange nicht die eigenen Daten in der Ransomware-Falle stecken. Ein weiteres Argument ist die fehlende Garantie, dass die Kriminellen ihre Angriffe nicht wiederholen.

Die Entscheidung liegt allein bei den Geschädigten. Ihnen sei mitgegeben: Womöglich gibt es keine Alternative zur Zahlung des Lösegeldes. Besser wäre es aber, es würde erst gar nicht zu einer Forderung kommen. Denn bevor Ransomware ihre Arbeit aufnehmen kann, muss sie Kontakt zu einem Command and Control Server aufnehmen. Leistungsfähige Firewalls, wie die Sophos UTM, verhindern das. Einen zusätzlichen Schutz bieten Lösungen, wie die Sophos „Next Generation Enduser Protection“, die Endpoint-, Mobile- und Verschlüsselungstechnologie in sich vereint.

Hintergrundinformationen zum Schutz von Organisationen vor Ransomware finden Sie hier:
https://secure2.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/cryptolocker-cryptowall-remove-ransomware.aspx?cmp=701j0000000LOhOAAW

Kostenlose Testversionen finden Sie hier:
http://www.sophos.com/en-us/products/free-tools.aspx

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
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-40-484434
sophos@tc-communications.de