Hacker-Lexikon: Was ist Full Disk Encryption?

Autor: Kim Zetter.Kim Zetter Sicherheit

WIRED | 2016.07.02

Es gab in den letzten Jahren über die Verschlüsselung und was die FBI Bedingungen seine "Möchten Dark" Problem seine Unfähigkeit, die Kommunikation von Überwachungsziele viel Gerede zu lesen, weil mehr und mehr Daten verschlüsselt werden. Und während die End-to-End-Messaging-Verschlüsselung, die gesendeten Daten geschützt werden in Anwendungen wie WhatsApp viel Presse bekommen, es ist ein Problem, das ebenso eine ruhende Daten gilt. Die Art, die Full-Disk-Verschlüsselung ausgelegt ist, zu schützen.

Diese Art von Schutz haben erhebliche Aufmerksamkeit während der jüngsten FBI-Apple-Kampf um die geschützten Daten auf der San Bernardino-Shooter iPhone zu bekommen. In der Tat stellte sich ein ungewolltes Marketing-Coup für die Tech-Riesen zu sein, aus, Hervorhebung der Stärke des Verschlüsselungsschema des Unternehmens auf seinen mobilen Geräten gespeicherten Daten. Weder das FBI noch Apple könnte die Passwort-Sperre auf dem iPhone zu umgehen, ohne Lösen der Festplattenverschlüsselung von Apple auf die neuesten Versionen seiner Geräte beschäftigt.

Das ist offensichtlich nicht der Fall mit Android-Geräte. Eine Geschichte in dieser Woche zeigt, dass die Festplattenverschlüsselung in das Android-Betriebssystem kann mit Brute-Force-Angriffe-die gebrochen werden, um ein Skript beinhaltet die Verwendung von tausenden von Passwort Vermutungen an ein Gerät zu senden, um die richtige zu bestimmen, die die Verschlüsselung entriegelt.

Festplattenverschlüsselung, die auch als ganze Festplattenverschlüsselung bekannt ist, schützt die Daten, die auf einem Computer oder Telefon im Ruhezustand ist, im Gegensatz zu E-Mail und Instant-Messaging-Daten, die über ein Netzwerk auf der Durchreise ist. Wenn effektiv getan, er verhindert, dass unbefugte Personen, einschließlich Telefon und Computer-Hersteller selbst, von Daten auf einer Festplatte gespeichert zugreifen. Das bedeutet, dass, wenn Sie hinter Ihrem Laptop oder Handy zu verlassen in dem Auto Über-Fahrer, oder einige unsteten Regierungsagent versucht, Ihren Computer an einem Flughafen oder einer anderen Grenzübergang zu gelangen, werden sie an Ihre Daten zu bekommen, ohne Ihre Hilfe- nicht in der Lage sein, selbst wenn sie auf die Festplatte und legen sie sie in einer anderen Maschine zu entfernen.

Festplattenverschlüsselung kommt in allen wichtigen kommerziellen Betriebssystemen gebaut; ein Benutzer einfach zu entscheiden, es zu benutzen und ein starkes Passwort oder eine Phrase zu wählen. Um ein System mit Festplattenverschlüsselung gesperrt zuzugreifen, wird der Benutzer aufgefordert, nach dem Einschalten des Geräts, aber bevor es vollständig bootet, um das Passwort oder einen Satz eingeben. Bei der Eingabe entsperrt das Kennwort einen Verschlüsselungsschlüssel in das System, das wiederum das System entriegelt, und gibt Ihnen Zugriff auf sie und Ihre Dateien. Einige Festplattenverschlüsselung Systeme erfordern Zwei-Faktor-Authentifizierung, die den Benutzer auffordert, ein Passwort einzugeben, nicht nur, sondern eine Smartcard in ein Lesegerät an den Computer angeschlossen zu rutschen, oder eine Reihe zufällig von einem Sicherheitstoken generiert ein.

Festplattenverschlüsselung unterscheidet sich von Datei in Verschlüsselung, dass diese verschlüsselt nur einzelne Dateien, die Sie für die Verschlüsselung angeben. Festplattenverschlüsselung schützt alle Daten auf einem System, einschließlich des Betriebssystems. Aber es schützt nur das System, während es ausgeschaltet ist. Sobald ein berechtigter Benutzer meldet sich bei dem Computer, entriegelt das die Festplattenverschlüsselung, zu verlassen ausgesetzt Daten und Systemdateien

jemand in der Lage, um den Computer zugreifen, während der Benutzer angemeldet ist, es sei denn, der Benutzer manuell einzelne Dateien als auch verschlüsselt. Es schützt auch nicht-Systeme von von Hackern über das Internet angegriffen zu werden. Es schützt nur gegen jemanden, der den physischen Zugriff auf das Gerät erhält.

Selbst dann ist es nicht unbedingt gepanzert. Ein Verschlüsselungssystem arbeitet nur als auch das Design. Ein System, das eine schwache Verschlüsselung oder, verwendet enthält Schwachstellen, wie es verschlüsselt die Festplatte ein falsches Gefühl der Sicherheit. Die jüngste Android Verwundbarkeit verdeutlicht dieses Problem. Flaws im Kernel des Betriebssystems Android-und im Qualcomm-Prozessor in Millionen von Android verwendet Geräte-untergraben die Android Plattenverschlüsselungssystem.

Dennoch beiseite gelegentliche Schwachstellen, ist Festplattenverschlüsselung eines der wichtigsten Werkzeuge in die Daten auf Ihren Geräten zu sichern.

Zurück zum Anfang. Wechseln zu: Anfang des Artikels.

lesen: https: //www.wired.com/2016/07/hacker-lexicon-full-disk-encryption/