Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Informatiksteuerungsorgan Bund ISB
Informatiksicherheit SEC

Rolf Oppliger
Hans Oppliger

19. November 2012

Technologiebetrachtung

„Pass-the-Hash“-Angriffe

1 Einleitung

„Pass-the-Hash“-Angriffe stellen eine grosse Gefahr für die Sicherheit von Firmennetzen dar. Die Angriffe setzen bei Passwort-basierten Authentifikationsverfahren an und nutzen insbesondere die Tatsache aus, dass ein Passwort vom Benutzer oft nur einmal eingegeben werden muss, danach aber in gehashter Form weiterverwendet werden kann. Das bedeutet, dass aus der Sicht des Angreifers die Kenntnis eines Passwort-Hashwertes äquivalent ist zur Kenntnis des entsprechenden Passwortes[1], bzw. dass aus dem Hashwert nicht vorgängig das Passwort ermittelt werden muss. Das vereinfacht Angriffe erheblich und macht sie insbesondere auch resistent gegenüber „gut gewählten“ Passwörtern (d.h. Passwörter mit hoher Entropie).

Im Rahmen dieser Technologiebetrachtung wird aufgezeigt, was ein „Pass-the-Hash“-Angriff ist, wie er funktioniert, wie gross das Gefährdungspotential ist und was man allenfalls dagegen tun kann.

2 Problematik

Ein „Pass-the-Hash“-Angriff läuft schematisch in den folgenden fünf Schritten ab:

- In Schritt 1 verschafft sich ein Angreifer die Berechtigungen eines lokalen Systemadministrators auf einem (oder mehreren) Client(s). Dazu kann er auf bekannte Angriffsvektoren zurückgreifen, wie z.B. den Versand von Spam-Mails mit HTTP-Links auf Web-Seiten, auf denen eine „Drive-by“-Infektion durchzuführen versucht wird.
- In Schritt 2 nutzt der Angreifer die Berechtigungen des lokalen Systemadministrators, um den (oder die) Client(s) zum Abgreifen von Passwort-Hashwerten vorzubereiten (z.B. durch Installation einer entsprechenden Malware).
- In Schritt 3 erzeugt der Angreifer auf einem so vorbereiteten Client einen Support-Fall und meldet diesen der dafür zuständigen Stelle (z.B. Help-Desk).
- In Schritt 4 loggt sich ein Supporter lokal oder über eine Terminalverbindung auf dem Client ein, um sich dem Fall anzunehmen. Verfügt der Supporter über die Be-

[1] In der einschlägigen Literatur wird dafür der Begriff „plaintext equivalent“ verwendet, d.h. der Passwort-Hashwert ist äquivalent zum Passwort im Klartext.

rechtigungen eines Domänenadministrators, können die entsprechenden Passwort-Hashwerte vom Client abgegriffen werden.
- In Schritt 5 nutzt der Angreifer diese Passwort-Hashwerte, um sich als Domänenadministrator anzumelden und die Kontrolle über die Domäne zu übernehmen.

Natürlich kann ein „Pass-the-Hash“-Angriff auch direkt gegen einen von einem Domänenadministrator verwendeten Client durchgeführt werden (wenn ein solcher bekannt und zugänglich ist). Die Schritte 1 – 4 erübrigen sich dann. So oder so ist es einem Angreifer oft möglich, binnen Stunden die Kontrolle über ganze Domänen und Forests zu erlangen.

Obwohl „Pass-the-Hash“-Angriffe vor allem Windows-basierte Firmennetze betreffen und in diesem Zusammenhang diskutiert werden, sind derartige Angriffe grundsätzlich in allen Netzen möglich, in denen sich Benutzer nicht ständig wieder neu authentifizieren müssen, sondern Credentials (z.B. in Form von Passwort-Hashwerten) lokal abgelegt und für Authentifikationsprozesse wiederverwendet werden. Entsprechend ist das zugrunde liegende Problem tiefgreifend und nicht durch Patchen von Software oder einfache Umgestaltung von Authentifikationsprozessen lösbar.

3 Lösungsansätze

In der Literatur werden zuweilen Lösungsansätze vorgeschlagen, die im Hinblick auf „Pass-the-Hash“-Angriffe nichts oder nicht viel bringen. So schützt z.B. der aus der UNIX-Welt bekannte „Salt“-Mechanismus zwar vor Offline-Wörterbuchangriffen aber nicht vor „Pass-the-Hash“-Angriffen. Das Gleiche gilt für „gut gewählte“ Passwörter, d.h. Passwörter mit hoher Entropie. Aus der Sicht eines „Pass-the-Hash“-Angriffs spielt die kryptografische Güte eines Passwortes keine Rolle, d.h. der Angriff funktioniert bei Trivialpasswörtern ebenso gut wie bei Passwörtern, die sehr lang sind und sich aus Zeichen speziell grosser Alphabete zusammensetzen. Auch höherwertige Benutzerauthentifikationsverfahren z.B. auf der Basis von Smartcards oder Biometrie nützen meist nicht viel, weil die Hashwerte der Benutzerpassworte lokal installiert und dort abgegriffen werden können. Schliesslich können kommerzielle Antivirenprogramme meist nur bekannte Malware erkennen, so dass der Angreifer die in den Schritten 1 und 2 verwendete Malware modifizieren und dadurch für Antivirenprogramme nicht erkennbar machen kann.

„Pass-the-Hash“-Angriffen, wie wir sie heute kennen, liegen zwei hauptsächliche Probleme zugrunde bzw. werden dadurch ermöglicht:

- Zum einen werden in Schritt 4 zur Behandlung des Support-Falles die Berechtigungen eines Domänenadministrators benötigt. Dazu werden die Hashwerte der entsprechenden Passwörter auf dem Client installiert, wo sie mit Hilfe vorgängig installierter Malware abgegriffen werden können.
- Zum anderen ist es für heute üblicherweise eingesetzte Authentifikationsprotokolle ausreichend, über einen Passwort-Hashwert (anstelle eines Passwortes) zu verfügen. Dies gilt namentlich für die LAN Manager (LM) und NTLM-Authentifikationsprotokolle, die trotz bekannter Schwächen aus Gründen der Rückwärtskompatibilität immer noch verbreitet im Einsatz stehen[2].

Ein Angreifer, der sich aufgrund des erstgenannten Problems den Hashwert eines Passwortes eines Domänenadministrators verschafft hat, kann sich aufgrund des

[2] Diese Aussage gilt auch für NTLM Version 2 (NTLMv2), d.h. NTLMv2 beseitigt zwar bekannte Verwundbarkeiten und Schwachstellen der LM- und NTLMv1-Authentifikationsprotokolle, in Bezug auf den Schutz vor „Pass-the-Hash“-Angriffen bringt aber NTLMv2 keine wesentliche Verbesserung.

zweitgenannten Problems gegenüber einem Domänencontroller authentifizieren und so die Kontrolle der Domäne übernehmen.

Will man „Pass-the-Hash“-Angriffe wirksam verhindern, kann man grundsätzlich bei beiden Problemen ansetzen, wobei in beiden Fällen eine Lösung schwierig ist.

- Im ersten Fall liegt die Schwierigkeit darin, dass ein Supporter über die Berechtigungen eines Administrators verfügen muss, um überhaupt sinnvolle Supportaufgaben ausführen zu können. Eine Beschränkung der Berechtigungen führt hier dazu, dass die Supportleistung für die betroffenen Benutzer unbefriedigend ausfallen muss. Zudem kann ein Angreifer immer aufwändigere Support-Fälle erzeugen, so dass irgendeinmal zu dessen Bewältigung die Berechtigungen eines Domänenadministrators erforderlich ist.
- Im zweiten Fall würde eine Lösung darin bestehen, dass der Benutzer entweder bei jeder Authentifizierung sein Passwort neu eingeben muss und dieses für die Authentifizierung eingesetzt wird oder er das Passwort nur einmal eingibt und dieses sicher (d.h. nicht auslesbar) zwischengespeichert wird. Beide Alternativen haben gravierende Nachteile: Die erste Alternative ist für den Benutzer unangenehm, weil er sein Passwort wiederholt eingeben muss. Die zweite Alternative hat das Problem, dass das Passwort sicher zwischengespeichert werden muss und es – wie die „Pass-the-Hash“-Angriffe zeigen – a priori nicht klar ist, wie dies bewerkstelligt werden kann.

Vor diesem Hintergrund empfiehlt Microsoft zum Schutz vor „Pass-the-Hash“-Angriffen verschiedene Massnahmen, die letztlich alle darauf abzielen, entweder mit den Berechtigungen von lokalen System- und Domänenadministratoren sparsam umzugehen oder sie zeitlich zu beschränken. Das ist aus sicherheitstechnischer Sicht sicherlich ein richtiger und sinnvoller Ansatz; leider kollidiert er in der Praxis mit betrieblichen Anforderungen, d.h. die Verwaltbarkeit einer Domäne kann leiden, wenn man die Berechtigungen von Administratoren allzu zu stark einengt und begrenzt.

Natürlich kann man auch den Standpunkt vertreten, dass man anstelle einer Supportdienstleistung einen betroffenen Client in jedem Fall neu aufsetzt. In diesem Fall greift der „Pass-the-Hash“-Angriff nicht und der Angreifer muss dann explizit einen von einem Domänenadministrator benutzten Client angreifen (um an den Hashwert eines Passwortes dieses Administrators zu gelangen). Wenn man diese Clients in einer separaten Domäne oder möglicherweise sogar in einem separaten Forest betreibt und die Kommunikationsmöglichkeiten auf das absolut Notwendige beschränkt, kann man das Verwundbarkeitsfenster klein halten.

4 Schlussfolgerungen und Ausblick

„Pass-the-Hash“-Angriffe stellen heute vor allem in Windows-basierten Firmennetzen ein grosses Problem mit einem erheblichen Gefährdungspotential dar. Die Angriffe sind möglich, weil Benutzer sich nicht permanent wieder neu authentifizieren wollen und stattdessen Credentials (z.B. in Form von Passwort-Hashwerten) lokal abgelegt und für Authentifikationsprozesse wiederverwendet werden. Solange an diesem „Single Sign-On“-Ansatz festgehalten wird, können „Pass-the-Hash“-Angriffe nicht wirksam verhindert, sondern nur in Bezug auf ihre Auswirkungen abgeschwächt werden. Durch eine Beschränkung der Berechtigungen von lokalen System- und Domänenadministratoren kann man versuchen, die Verwundbarkeitsfenster klein zu halten. Natürlich ist das nicht nachhaltig, weil auch ein kleines Fenster für einen versierten Angreifer zur Übernahme einer Domäne genutzt werden kann. Alternativ kann man anstelle von Supportdienstleistungen auch Clients in Problemfällen neu aufsetzen oder die lokalen Systemadministratorenkonti deaktivieren. Letz-

teres verhindert zwar das Installieren von Malware zum Angreifen von Passwort-Hashwerten, es verhindert aber nicht notwendigerweise andere Angriffsvektoren zum Abgreifen der Passwort-Hashwerte (z.B. direktes Auslesen aus dem Hauptspeicher).

Theoretisch könnte ein alternativer Lösungsansatz darin bestehen, dass man sich vom „Single Sign-On“ (SSO) verabschiedet und von den Benutzern stattdessen verlangt, dass sie sich häufig wieder authentifizieren (damit die Passwort-Hashwerte nicht lokal zwischengespeichert werden müssen). Das wäre allerdings für die Benutzer unangenehm und entsprechend unwahrscheinlich ist es, dass sich ein solcher Ansatz durchsetzen wird. Mit verschiedenen, zur Zeit laufenden Initiativen für SSO ist tendenziell eher mit einem Anstieg von „Pass-the-Hash“-Angriffen in Firmennetzen und damit mit einer Verschärfung der Problematik zu rechnen. In einem gewissen Sinn stellen „Pass-the-Hash“-Angriffe den Preis dar, den man für SSO zu bezahlen bereit sein muss. Nichtsdestotrotz wird man nicht umhin kommen, die Privilegien und Aktivitäten von lokalen System- und Domänenadministratoren besser zu überwachen und mit Hilfe von heuristischen Verfahren zu kontrollieren.

Zu guter Letzt darf vermerkt werden, dass vom Betriebssystem unabhängige Datei-basierte Verschlüsselungsmechanismen und -produkte grundsätzlich resistent gegenüber „Pass-the-Hash“-Angriffen sind, d.h. wenn ein Benutzer bestimmte Dateien verschlüsselt hat und die entsprechenden Schlüssel nicht im Klartext auf dem Client vorliegen, kann ein Angreifer, der sich mit Hilfe eines „Pass-the-Hash“-Angriffs die Berechtigungen eines Domänenadministrators verschafft hat, diese Daten auch nicht lesen. Das ist deshalb wichtig, weil viele Angriffe heute darauf abzielen, nach der Kompromittierung eines Clients möglichst viele Dateien weg zu kopieren. Bei Container-basierten Verschlüsselungsmechanismen und -produkten ist dies einfach möglich, weil die Container mit grosser Wahrscheinlich geöffnet sind, während es bei Datei-basierten Verschlüsselungsmechanismen und -produkten nur dann möglich ist, wenn der Benutzer auf die Dateien zugreift.