Een goed wachtwoord is niet alleen lang, maar ook complex

Opinie

Het kiezen van een lang wachtwoord zou meer veiligheid bieden dan het kiezen van een complex wachtwoord, concludeerde columnist Roger Grimes onlangs. Hugo Leisink vindt die conclusie onjuist en het in de praktijk brengen ervan zelfs gevaarlijk.

De Amerikaanse columnist Roger A. Grimes concludeerde onlangs dat het kiezen van een lang wachtwoord meer veiligheid biedt dan het kiezen van een complex wachtwoord. Het artikel is te vinden via: *www.infoworld.com/article/06/07/21/30OPsecadvise_1.html*. Het eerste dat opvalt is dat slechts drie wachtwoorden gebruikt zijn tijdens Grimes' onderzoek. Dit maakt naar ons idee de kans op een toevalligheid van de kraaktijden niet verwaarloosbaar klein. We zijn daarom van mening dat uit het onderzoek een te snelle conclusie is getrokken.

Het eerste wachtwoord uit het onderzoek (S1owDr1v3r) bevat hoofdletters, kleine letters en cijfers. Per positie in het wachtwoord zijn er dus 62 mogelijkheden. Met een wachtwoord van 10 tekens komt het aantal mogelijke wachtwoorden op 62^{10} = 839.299.365.868.340.224.

Het tweede wachtwoord uit het onderzoek (myengagingwifes) bestaat slechts uit kleine letters (26 tekens) en is 15 tekens lang. Dit geeft een aantal van 26^{15} = 1.677.259.342.285.725.925.376 mogelijke wachtwoorden. Een bruteforce-aanval op dit wachtwoord zal gemiddeld genomen aanzienlijk meer tijd in beslag nemen dan op het eerste wachtwoord, omdat van het tweede wachtwoord meer combinaties te maken zijn. Dit is in lijn met het resultaat van Grimes' onderzoek.
Maar als we het tweede wachtwoord bekijken, dan zien we dat dit uit drie aan elkaar geplakte woorden bestaat. Dit wachtwoord is vergelijkbaar met een wachtwoord bestaande uit drie tekens waarbij ieder teken een aantal mogelijkheden heeft dat even groot is als het aantal woorden uit de gekozen taal, Engels in dit geval. Een gemiddelde woordenlijst voor het kraken van wachtwoorden bestaat uit ongeveer 60.000 woorden (de in het tweede wachtwoord gebruikte woorden zijn aanwezig in de woordenlijsten die op internet te vinden zijn). Het aantal combinaties komt dan op 'slechts' 60.000^3 = 216.000.000.000.000.

REAGEREN?
Geef uw mening op http://re.ageer.nu

Het interessante aan een wachtwoord in de vorm van een zin is dat we te maken hebben met een entropie die lager is dan het maximaal mogelijke. Met entropie bedoelen we hier de willekeurigheid van de woorden in het wachtwoord. Deze is lager door het gebruik van grammaticaregels. Immers, in een normale Nederlandse of Engelse zin wordt bijvoorbeeld een bijvoeglijk naamwoord nooit achter een zelfstandig naamwoord geplaatst. Het aantal waarschijnlijke combinaties voor het tweede wachtwoord kan dus omlaag gebracht worden door het wachtwoordkraakprogramma de grammaticaregels te leren.

Dat het eerste wachtwoord eerder geraden is dan het tweede wachtwoord zegt naar ons idee dan ook meer over de gebruikte wachtwoordkraaktechnieken dan over de sterkte van de gekozen wachtwoorden. Als gebruikers daadwerkelijk langere wachtwoorden bestaande uit slechts kleine letters gaan gebruiken en kwaadwillenden hun kraakprogramma's daarop aanpassen, zijn gebruikers alleen maar slechter af. De conclusie uit het onderzoek is daarom ook nog eens gevaarlijk.

De sterkte van een wachtwoord is enkel en alleen afhankelijk van de tijdsduur die nodig is om het wachtwoord middels bruteforce-technieken te kraken. Alle overige zaken, zoals het gebruikte hashing-algoritme (MD5, SHA1, et cetera) of de mogelijkheid tot afluisteren, zeggen niets over de sterkte van het wachtwoord zelf, maar over de veiligheid van de opslag en transport van het wachtwoord en laten we daarom buiten beschouwing. De tijdsduur voor het kraken is afhankelijk van het aantal wachtwoorden dat geprobeerd moet worden. Dit aantal mogelijke wachtwoorden is weer afhankelijk van:

1. De lengte van het wachtwoord
2. Het aantal gebruikte tekens in het wachtwoord
3. De entropie van de gebruikte tekens.

Dit laatste kan als volgt in normaal Nederlands worden opgeschreven: Een veilig (sterk) wachtwoord is een wachtwoord dat niet te kort is (neem meer dan 8 tekens), een groot aantal mogelijke tekens bevat (neem naast letters ook cijfers en leestekens op in het wachtwoord) en waarbij er geen verband bestaat tussen het ene teken en het andere teken (vermijd het gebruik van namen en woorden in het wachtwoord).

WGDJ#14DN&SOV GOED TE ONTHOUDEN, NIET TE KRAKEN

Een goede en handige methode voor het kiezen van een veilig wachtwoord is het nemen van een willekeurige zin die makkelijk te onthouden is. Uit die zin worden de beginletters van ieder woord genomen, aangevuld met wat leestekens. Kies bij voorkeur een zin waar een getal in voorkomt. Voorbeeld: Wij gaan dit jaar 14 dagen naar Spanje op vakantie. Het wachtwoord wordt dan: Wgdj#14dn&Sov
Met deze methode voldoet het wachtwoord aan de drie bovengenoemde eisen voor een veilig wachtwoord en is het ook nog makkelijk te onthouden.

HUGO LEISINK
AG • 15-06-'07

Hugo Leisink is Internet Security Consultant bij Vanveen informatica bv.