WEGWERPWACHTWOORDEN EN TWEEFACTORAUTHENTICATIE

NOG VEILIGER MET EEN YUBIKEY

TEKST: **KOEN VERVLOESEM**

Onveilig opgeslagen wachtwoorden van allerlei internetdiensten komen regelmatig op straat te liggen. Twee manieren om zo'n gelekte wachtwoordlijst onbruikbaar te maken zijn wegwerpwachtwoorden en tweefactorauthenticatie. Met de YubiKey zijn beide manieren eenvoudig toe te passen. In dit nummer van PC-Active kunt u voordelig een YubiKey aanschaffen; hier leest u hoe u hem optimaal benut.

Het is de zwakke plek van het klassieke wachtwoord: als het wordt gestolen of afgeluisterd, kan iemand zich voor u uitgeven. Een alternatief vormen zogenoemde one-time passwords (OTP), die - zoals de naam al aangeeft - maar één keer geldig zijn. Het zijn als het ware wegwerpwachtwoorden: u gebruikt dit password één keer en daarna is het niet meer geldig. Staat er een keylogger op uw computer of onderschept iemand op een andere manier uw wachtwoord, dan kan hij of zij hier niets mee doen. Zodra u het wachtwoord hebt ingegeven, is het immers geen tweede keer meer bruikbaar.

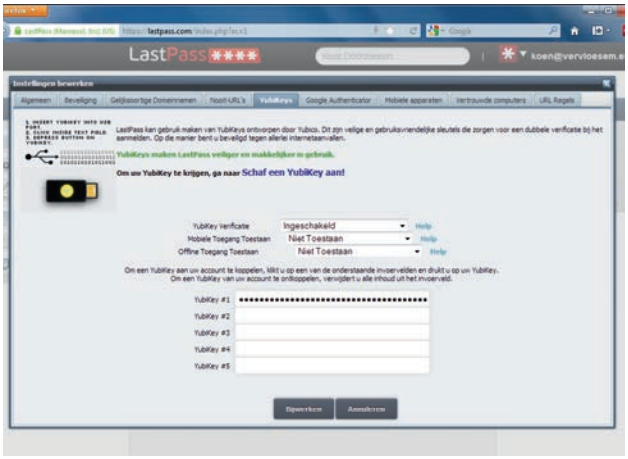
Slimme cryptografie

Maar hoe worden zulke wegwerpwachtwoorden dan aangemaakt? Daar zit heel wat slimme cryptografie achter, meestal in combinatie met een hardware-dongle. Dat apparaatje genereert telkens een nieuw wegwerpwachtwoord, en de dienst waarbij u zich aanmeldt kan verifiëren of dit wachtwoord door uw dongle is gegenereerd. Bovendien heeft elk wegwerpwachtwoord ook een volgnummer en houdt de dienst in een databank bij welke van die nummers reeds zijn gebruikt. Als u eenmaal met een wegwerpwachtwoord bent ingelogd, is het systeem dan ook onverbiddelijk: iemand die het wachtwoord heeft onderschept, kan het niet gebruiken om binnen te komen. Hoe de techniek van deze zogeheten one-time passwords werkt, zullen we uitleggen in de rubriek Denkwerk van volgende maand.

Er bestaan heel wat types dongle met deze functionaliteit, zoals RSA Security's SecurID of Vasco's DigiPass. Een minder bekende maar heel flexibele oplossing, die ook al heel wat referenties heeft, is de YubiKey [1] van het Zweedse bedrijf Yubico [2].

Het is een USB-sleutel die u in uw computer steekt en die voorzien is van een knop. Elke keer dat u op de knop drukt, stuurt de YubiKey een unieke sleutel naar de computer. Het mooie van dit alles is dat het op alle besturingssystemen zonder drivers werkt. De YubiKey doet zich immers voor als een USB-toetsenbord. Het kleinood weegt slechts 2,5 gram en u kunt het gerust aan uw sleutelbos hangen. Voor nog geen twintig euro hebt u een YubiKey, maar er is ook een compacte versie (YubiKey Nano, 1,5 g) en een contactloze versie (YubiKey NEO).

Deze laatste maakt gebruik van Near Field Communication, een draadloze standaard die bijvoorbeeld ook in sommige smartphones is ingebouwd. U hoeft de YubiKey dan slechts even bij uw smartphone te houden om uw wegwerpwachtwoord in te voeren. Het werkt eigenlijk net zoals de ov-chipkaart.



U kunt één of meer YubiKeys aan LastPass toevoegen om de toegang te beveiligen

Tweefactorauthenticatie

De veiligste authenticatiemanier om een YubiKey te gebruiken is in combinatie met een gebruikersnaam en een klassiek wachtwoord. Zo bereikt u immers een vorm van tweefactorauthenticatie: een combinatie van iets wat u weet - gebruikersnaam en wachtwoord - en iets wat u hebt, de YubiKey. Iemand die de ene factor - uw gebruikersnaam en wachtwoord - onderschept, kan dan nog altijd niet op de dienst inloggen, omdat u ook een eenmalig wachtwoord van de YubiKey moet ingeven. Het is bovendien niet genoeg zo'n eenmalig wachtwoord te onderscheppen. En iemand die enkel de andere factor - uw YubiKey - te pakken heeft gekregen, kan ook niet inloggen, omdat hij of zij daarnaast uw gebruikersnaam en wachtwoord moet weten.

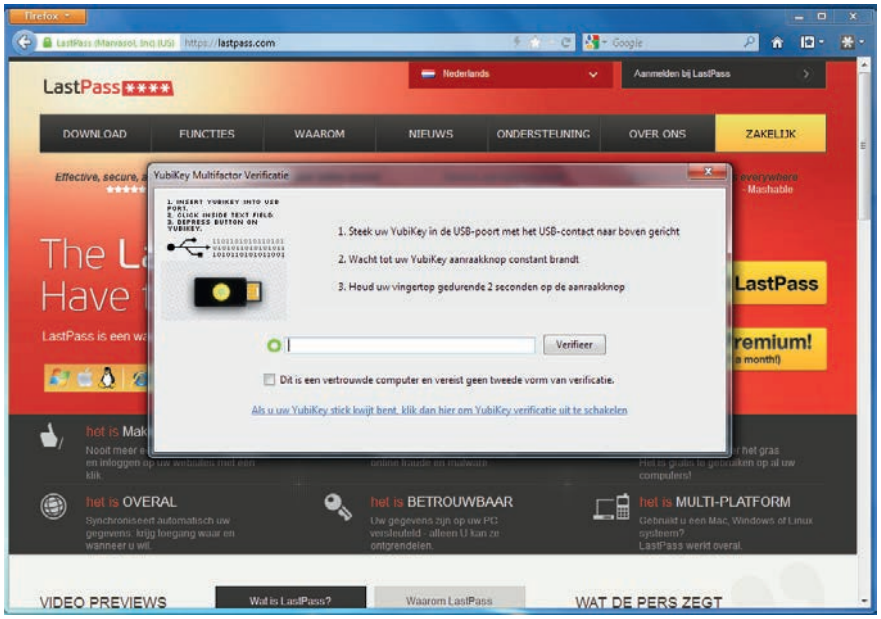
Wachtwoordkluis

Een tool zoals de YubiKey gebruikt u natuurlijk niet bij elke dienst waar u zich moet aanmelden, want het blijft iets omslachtiger dan enkel een gebruikersnaam en wachtwoord ingeven. Maar de YubiKey is erg geschikt om een wachtwoordkluis mee te beveiligen.

In plaats van het groeiend aantal wachtwoorden voor allerlei websites en andere diensten zelf te onthouden - wat bijna onmogelijk is, want een goed wachtwoord is per definitie moeilijk te onthouden - gebruikt u hopelijk een wachtwoordkluis, een programma dat al uw wachtwoorden voor u onthoudt. Die kluis - eigenlijk een bestand met uw wachtwoorden - wordt dan versleuteld, en de YubiKey is een goede extra beveiligingslaag. U wilt natuurlijk niet dat al uw wachtwoorden op straat komen te liggen door een slechte beveiliging van uw wachtwoordkluis, dus de extra stap naar tweefactorauthenticatie - zie ook het kader - is in dit geval niet overdreven.

Eén van die wachtwoordkluizen die u met de YubiKey kunt integreren is LastPass [3], al wordt het sleuteltje enkel in de betaalde Premium-variant ondersteund. De prijs van twaalf dollar per jaar is echter niet overdreven als u daarvoor wat gemoedsrust koopt. Installeer hiervoor eerst LastPass - dat overigens niet enkel voor Windows bestaat - dat browserextensies voor Internet Explorer, Firefox, Chrome, Safari en Opera installeert. Na de installatie vervangt LastPass het wachtwoordbeheer van uw webbrowser. U krijgt op het einde ook de vraag om een LastPass-account aan te maken. Geef nu een sterk hoofdwachtwoord op waarmee uw wachtwoordkluis wordt versleuteld.

Wanneer u uw LastPass-account een Premium-upgrade hebt gegeven, klik dan op uw profielpagina links op Instellingen en kies het tabblad YubiKeys. Verander YubiKey Verificatie in Ingeschakeld. Daaronder staan twee instellingen die het gebruik van de YubiKey in specifieke omstandigheden uitsluiten: als u een mobiel apparaat met de LastPass-app gebruikt - smartphones hebben normaal gesproken geen USB-aansluiting om de YubiKey te gebruiken - en als u LastPass offline gebruikt; de verificatie van het wegwerpwachtwoord van uw YubiKey vereist immers een online verbinding met Yubico's server. Beide instellingen kunt u het beste op Niet Toestaan zetten, tenzij u de beveiliging in deze gevallen bewust wilt kunnen omzeilen.



Uw wachtwoordkluis blijft gesloten voor wie uw YubiKey niet heeft

Om nu uw YubiKey aan uw account te koppelen is het voldoende om de cursor in één van de vijf grote invoervelden te plaatsen en met een druk op de knop van uw YubiKey een wegwerpwachtwoord in te geven. U kunt dus tot vijf YubiKeys aan uw account koppelen. Klik tot slot op Bijwerken en geef het hoofdwachtwoord van LastPass in. Wanneer uw YubiKey eenmaal is toegevoegd, log dan uit LastPass uit en opnieuw in, en dat in alle webbrowsers waarin u de LastPass-extensie gebruikt. De lokale cache van uw wachtwoordkluis wordt dan immers opnieuw versleuteld. Vanaf nu kunt u zich pas bij LastPass aanmelden - en dus van uw wachtwoordkluis gebruikmaken - na het invoeren van uw hoofdwachtwoord én een wegwerpwachtwoord van uw YubiKey.

API-sleutel

Een aantal toepassingen dat de YubiKey gebruikt, vereist een API-sleutel. Deze maakt u aan op de website van Yubico [4]. Vul in het formulier uw e-mailadres in en een door uw YubiKey gegenereerd wegwerpwachtwoord. De webpagina toont u dan een client-ID en een API-sleutel ('Secret key'), die u in allerlei toepassingen nodig hebt. Noteer beide gegevens en hou zeker de API-sleutel geheim.

Aanmelden in Windows

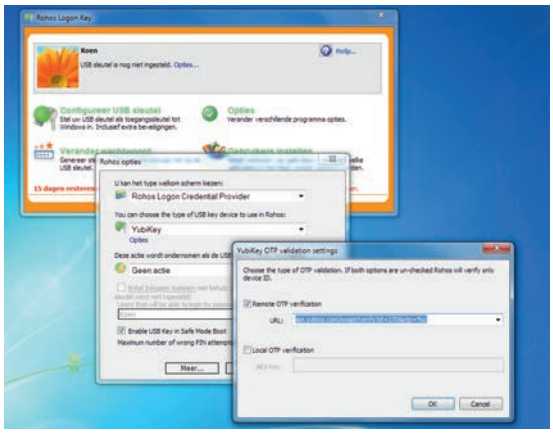
U kunt de YubiKey ook gebruiken om uw Windows-account mee te beveiligen. Als u bang bent dat uw collega's of huisgenoten u wel eens bespieden om uw wachtwoord te weten te komen, dan kunt u het best instellen dat het aanmeldscherm naast uw wachtwoord ook een wegwerpwachtwoord van uw YubiKey vereist. Er zijn verschillende programma's die deze functionaliteit aanbieden.

Rohos Logon Key [5] ondersteunt de YubiKey voor tweefactorauthenticatie bij de Windows-login, zij het enkel in de betaalde versie à 25 euro. Twijfelt u eraan of het een geschikte oplossing voor u is, dan kunt u vijftien dagen lang een volledig functionele trialversie van het programma uitproberen.

Klik in het hoofdvenster van het programma op Opties en kies YubiKey bij het type USB-sleutel. Klik daaronder dan op het blauwe woord Opties dat verschijnt en vink 'Remote OTP verification' aan. Kies in het dropdownmenu de URL van Yubico, die er standaard staat, en vervang in de URL het getal dat achter *id=* staat door het client-ID dat u van Yubico heeft ontvangen bij het aanvragen van een API-sleutel; zie ook het kader 'API-sleutel'.

In de opties kunt u ook kiezen welke actie Rohos uitvoert wanneer u uw YubiKey uit de computer verwijdert. U kunt de computer dan laten uitschakelen of in slaapstand brengen, u kunt dan afmelden, uw scherm vergrendelen of de screensaver starten. Klik op OK om de opties te bevestigen. Klik daarna in het hoofdscherm op 'Configureer USB-sleutel'. Steek uw YubiKey in de computer, typ uw Windows-wachtwoord in en klik op 'USB-sleutel instellen'. Hierna vraagt Rohos u om een pin in te geven - een statisch wachtwoord - en in het veld daaronder op de knop van de YubiKey te drukken. Herstart hierna de computer, waarna Windows u naast uw pincode om een druk op de YubiKey vraagt om aan te melden. Hebt u dat gedaan, open dan weer het hoofdvenster van Rohos Logon Key en vink 'Enkel Inloggen toelaten met behulp van USB-stick' aan, zodat u niet om het gebruik van de YubiKey heen kunt. U kunt hier ook ingeven welke gebruikers met alleen hun Windows-wachtwoord blijven aanmelden als niet iedere gebruiker tweefactorauthenticatie nodig heeft.

Tot slot kunt u ook een noodlogin instellen voor als u uw YubiKey verliest, maar let hiermee op, want



Met Rohos Logon Key beveiligt u de toegang tot uw Windows-account met een YubiKey

het programma geeft voorbeeldvragen waarop het antwoord nogal eenvoudig is te raden, zoals: "Wat is je favoriete automerk?"

Yubico heeft ook zelf een oplossing om de YubiKey voor tweefactorauthenticatie bij een Windows-login te gebruiken: de Yubico Windows Login tool [6], open source-software die gratis is te gebruiken. Dit is echter nog een bètaoplossing en vereist dat u uw YubiKey in slot 2 configureert voor een HMAC-SHA1 challenge-response; zie ook het kader 'Herprogrammeer uw YubiKey'. Voor bedrijfsomgevingen is er ook AuthLite [7] van Collective Software, dat is geïntegreerd met Active Directory.

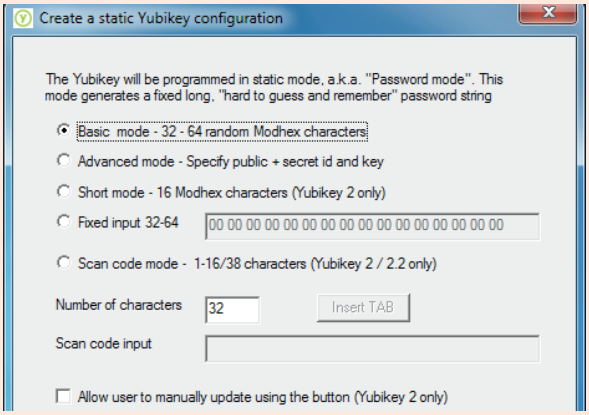
En verder

We lieten in dit artikel zien hoe u met een YubiKey uw wachtwoordkluis en Windows-account beter afschermt, maar er zijn nog veel meer mogelijkheden. Dankzij de open source-softwarebibliotheken die Yubico heeft vrijgegeven, hebben al heel wat webapplicaties ondersteuning voor de YubiKey ingebouwd - zij het van huis uit, zij het na installatie van een plug-in. Voor WordPress bestaat er bijvoorbeeld een YubiKey-plug-in, maar ook Drupal en Joomla! zijn op deze manier te configureren om tweefactorauthenticatie aan te bieden, evenals de webmailsoftware RoundCube en SquirrelMail. En zelfs de tweefactorauthenticatie van Google Apps kunt u met een YubiKey implementeren. Al met al is de YubiKey dan ook een flexibele en veelzijdige oplossing voor veilige authenticatie.

Herprogrammeer uw YubiKey

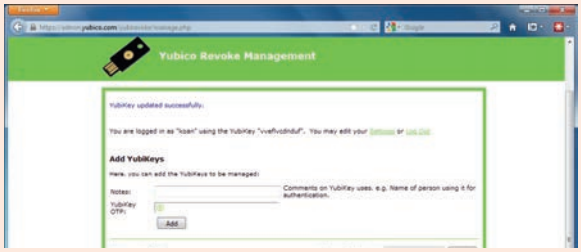
Yubico biedt op zijn website heel wat tools en softwarebibliotheken aan om de YubiKey te herprogrammeren - YubiKey Personalization Tools [8] - zowel voor Windows als voor OS X en Linux, inclusief uitgebreide documentatie. Voor Windows is de YubiKey Configuration Utility het handigst. Hiermee kunt u de YubiKey in verschillende modi configureren. Vanaf versie 2, uit 2009, heeft de YubiKey twee slots die elk in een onafhankelijke modus kunnen worden ingesteld. In het eerste slot is standaard een wegwerpwachtwoord geconfigureerd dat met Yubico's servers samenwerkt, maar in het tweede slot kunt u een statisch wachtwoord configureren, een wegwerpwachtwoord volgens de OATH-HOTP-standaard of een HMAC-SHA1 challenge-response configuratie. Een statisch wachtwoord is bijvoorbeeld interessant als u een TrueCrypt-volume met een sterk wachtwoord wilt versleutelen, maar dit niet kunt onthouden. U laat de YubiKey (een deel van) dit wachtwoord dan ingeven, maar dan mag u het kleinood natuurlijk niet verliezen...

Het eerste slot kunt u ook herconfigureren, maar als u het dan nog met Yubico's servers wilt gebruiken - bijvoorbeeld voor LastPass - dan moet u de AES-sleutel van de YubiKey opnieuw uploaden, wat ook vanuit de YubiKey Configuration Utility gaat. De uitvoer van het tweede slot activeert u overigens door wat langer op de knop te drukken, terwijl de uitvoer van het eerste slot door een korte druk op de knop naar de computer wordt gestuurd.



Trek uw YubiKey in

Een YubiKey als extra beveiliging is handig, maar wat als u dat kleine USB-sleuteltje verliest? Dat is sneller gebeurd dan u denkt, want veel weegt het ding niet... Gelukkig heeft Yubico hieraan gedacht: als u van Yubico's servers gebruikmaakt voor authenticatie, bijvoorbeeld bij LastPass, maak dan een account aan voor de dienst YubiRevoke [9]. Hiervoor moet u ook een YubiKey gebruiken voor de authenticatie. Verlies deze niet, want hiermee beheert u het in- of uitschakelen van al uw andere YubiKeys! Daarna kunt u al uw YubiKeys toevoegen. Het is belangrijk dat u dit onmiddellijk doet nadat u ze hebt gekocht, nog voor u ze gebruikt, want als u uw YubiKey eenmaal hebt verloren, kunt u ze niet meer uitschakelen. Vink Enabled bij een YubiKey uit zodra u een sleutel hebt verloren, zodat anderen er geen misbruik meer van kunnen maken. Deze dienst werkt overigens niet om YubiKeys in te trekken die u in een andere modus hebt geherprogrammeerd.



INFOLINK 265000
Voor de voetnoten bij dit artikel:
http://www.pc-active.nl/265000

QR CODE NOG AANLEVEREN