



Identificatie en Authenticatiemechanismen

Hoe zorg je er voor dat de toegang tot gegevens, de toegang tot een gebouw of een specifieke ruimte alleen wordt verleend voor degenen die hier ook toe geautoriseerd zijn?

In het verleden was een identificatie en authenticatiemechanisme van gebruikersnaam en wachtwoord voor de meeste toepassingen in een organisatie voldoende om ongeautoriseerde inzage of erger, mutatie of verwijderen van gegevens te voorkomen.

Een toepassing was alleen toegankelijk via een werkplek in het bedrijf. De werkplekken stonden in een ruimte die in principe alleen toegankelijk was voor medewerkers. Op de werkplek was veelal voldoende sociale controle, zodat de risico's van ongeautoriseerde ontsluiting, mutatie of verwijderen van gegevens voldoende waren afgedekt.

Met de opkomst van het thuiswerken, het internet en de grote ontsluiting van gegevens naar zakelijke partners en andere belanghebbenden zijn bovengenoemde risico's veel groter geworden. Voor veel gegevens geldt dat deze vanaf elke gewenste plek benaderbaar zijn. Een identificatie en authenticatiemechanisme, alleen gebaseerd op gebruikersnaam en wachtwoord is veelal niet meer voldoende.

Daarbij komt nog dat door de opkomst van het internet het aantal wachtwoorden voor de gemiddelde gebruiker explosief is gestegen. Veel websites kennen een "mijnwebsite" gedeelte, waarbij een gebruikersnaam en wachtwoord noodzakelijk is. De kans is reëel dat je bij het onderscheppen van een wachtwoord van een persoon, je ook toegang hebt tot andere gegevens, zoals bedrijfstoepassingen., omdat men overal hetzelfde wachtwoord, soms in een aantal variaties, toepast.

Er zijn al jaren andere authenticatiemechanismen op de markt, die als sterker gelden, dat wil zeggen waarbij misbruik veel moeilijker is.

Een voorbeeld hiervan is de smartcard. Hoewel de smartcard in allerlei vormen een opmars heeft gemaakt, heeft deze toch niet voor een echte omslag gezorgd.

Ook is biometrie in opmars. Zo zal vanaf augustus dit jaar het Nederlandse paspoort worden voorzien van een chip met biometrische eigenschappen van de houder.

Hoewel authenticatie op basis van biometrie heel sterk lijkt zijn er toch steeds kritische geluiden te horen. Zo wil bijvoorbeeld de Rabobank om reden van acceptatie nog geen biometrische authenticatie invoeren. De ABN AMRO bank heeft proeven gedaan met stemherkenning als authenticatie, maar ook daar is lang niet iedereen onverdeeld positief over.

Ook zijn er kritische geluiden over privacy bescherming. In hoeverre zijn biometrische gegevens beschermd tegen misbruik?

Tegenstanders van biometrische authenticatie voeren aan dat, indien misbruik kan worden gemaakt, het vrijwel ondoenlijk is om aan te tonen dat iemand anders misbruik heeft gemaakt van jouw biometrische gegevens, juist omdat het vertrouwen in biometrische authenticatie bij overheden en instellingen hoog is. Ook zou, indien biometrische gegevens centraal worden opgeslagen, deze gegevens ook kunnen worden misbruikt voor andere doeleinden.



USB stick met fingerprint toegang.

Waarschijnlijk zullen we het nog even moeten doen met het vertrouwde wachtwoord. De verwachting is echter dat biometrische authenticatiemechanismen uiteindelijk het wachtwoord zal vervangen.

Updates programmatuur

Onlangs heeft Secure Connection BV StandardGUI aangepast. Zo is het met de huidige versie mogelijk om bij het maken van een lijst of een rapport direct het betreffende programma (Adobe Acrobat Reader of MS Word lokaal op te starten. Verder komt Secure Connection binnenkort met een autosave versie. Dit houdt in dat het antwoordobject regelmatig automatisch wordt opgeslagen.

Actueel

Onveilig internetten via NS hotspots?

Deze week kwamen berichten in de media dat gebruikers van het draadloos internet van de NS dit wekenlang op een onveilige manier hebben gedaan.

Roel Schouwenberg van Kaspersky heeft NS en KPN hierop geattendeerd en het gat zou inmiddels zijn gedicht. Wat was er aan de hand?

Het gebruik maken van een hotspot van de NS gaat tegen betaling. Bij het gebruik maken van de hotspot komt de gebruiker op een inlogsite van de NS. De verbinding tussen de inlogsite van de NS en de browser van de gebruiker liep gewoon over http in plaats van https. Hierdoor kon de communicatie tussen webbrower en inlogsite eenvoudig worden opgepakt door anderen. Zo kan username en wachtwoord voor toegang tot het internet via deze hotspot worden onderschept. Inmiddels wordt er doorgelinkt naar de KPN inlogsite die wel met https werkt. Het is niet zo dat op deze manier ook bijvoorbeeld betalingsverkeer kon worden onderschept, aangezien de banksites zelf wel gebruik maken van https.

Bron:

<http://www.bright.nl/kpn-bevestigt-ns-hotspots-waren-onveilig>