Inge Heuvel - van Schaijck --- Online

Van: Maarten Heuvel - Online <maarten@onlinegroep.nl>
Verzonden: maandag 13 maart 2017 13:30
Aan: info@onlinegroep.nl
Onderwerp: Online Pro Update 2017.0.0.30: HTTPS Beveiliging van de website / mijnpolissen-portal / OnlinePro-portal van Online Pro

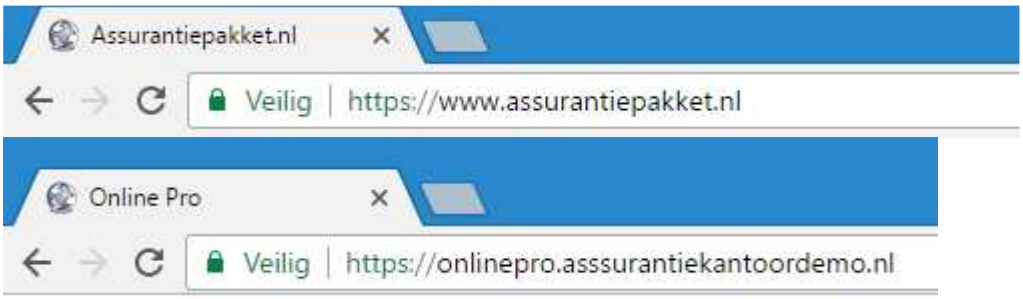
Beste Online Pro Gebruikers,

In de update van Online Pro van vandaag introduceren we een nieuwe dienst HTTPS beveiliging.

U kunt deze update ophalen door in het menu Systeem voor Synchroniseren te kiezen.

Hoe herkent u een veilige website?

U ziet in uw browser dan het woord "Veilig" staan of een slotje en de website-url begint met HTTPS.



HTTPS beveiliging

Het wordt tegenwoordig steeds vaker gevraagd dat websites "veilig" zijn (HTTPS) gezien de mogelijkheid op misbruik van gegevens door derden via HTTP.

Wat is de impact van een niet-HTTPS website in de praktijk?

U logt bijvoorbeeld op mijnpolissen.uwdoweinnaam.info of op onlinepro.uwdoweinnaam.info via een mobiele verbinding (ofwel Wi-Fi of 3G/4G/5G internet).
Iemand in de buurt van uw telefoon kan deze verbinding eenvoudig afluisteren met een extern apparaat. Uw telefoon/tablet of laptop denkt met het echte Wi-Fi of 3G/4G/5G punt verbonden te zijn maar is in werkelijkheid verbonden met een afluisterapparaat.
Gevolg is dat deze persoon alle informatie kan zien die u "onbeveiligd" via telefoon/tablet of laptop verstuurt.
Het gevoeligste zijn dan de **gebruikersnaam en wachtwoord** van de HTTP-website die opgevangen kunnen worden en later misbruikt wordt.

Tevens is dit op vaste computers met een vaste internetverbinding natuurlijk ook mogelijk. Zodra daar een programma op geïnstalleerd is geraakt wat e.e.a. afluistert, kan deze hier ook misbruik van maken. Met HTTPS voorkom je dit probleem.

Google en HTTPS

Ook grote organisaties als Google zijn het gebruik van HTTPS behoorlijk aan het promoten.
Google geeft aan de zoekresultaten van websites die niet HTTPS zijn lager in de ranking te plaatsen. Uw website wordt dus lager in de zoeklijst geplaatst als hiernaar gezocht wordt.

U wordt op deze manier minder vindbaar als uw site nog HTTP is.

Oplossing : HTTPS certificaat voor uw domeinnaam

De oplossing is dat u een HTTPS certificaat heeft voor uw domeinnaam (of namen) waarbij deze gebruikt wordt om alle diensten via HTTPS te laten verlopen.
Dit houdt het volgende in:
- HTTPS certificaat aanschaffen voor de duur van 3 jaar (verlenging na 3 jaar)
- Aanpassen websites door hostingprovider dat deze via HTTPS werkt.
- Eventueel aanpassen van uw huidige website indien deze links heeft naar HTTP://uweigendomeinnaam.nl
- Alle portals aanpassen en op HTTPS laten functioneren.

Het aanvragen van certificaten en technisch in de juiste formaten zetten voor de verschillende diensten/server systemen vereist aardig wat technische kennis en werkzaamheden.
Om dit voor u als tussenpersoon eenvoudig toegankelijk te maken hebben we hiervoor automatiseringssoftware geschreven die een deel van dit proces automatiseert. De rest van de handmatige werkzaamheden analyseren wij en voeren wij voor u uit.

Kosten omzetting naar HTTPS beveiliging.

De kosten voor de omzetting naar HTTPS zijn als volgt opgebouwd:
- Aanvraag & verwerkingskosten € 170,- incl. btw voor 3 jaar.
- Per domeinnaam € 30,- incl. btw voor 3 jaar.

Voorbeeld:
Indien u de website **www.uwkantoor.nl** bij ons heeft lopen en de 2 portals wilt beveiligen **OnlinePro.uwkantoor.nl** en **MijnPolissen.uwkantoor.nl** zijn de kosten als volgt:
- Aanvraag & verwerkingskosten € 170,-
- 3 Domeinnamen a € 30,- = € 90,-
- Total € 260,- incl. btw voor 3 jaar HTTPS beveiliging van uw websites.

Geïnteresseerd in HTTPS beveiliging van uw website?

Stuur een reply op deze e-mail met de domeinnaam (of namen) die u beveiligd zou willen hebben. Wij nemen dan contact met u op om e.e.a. door te nemen.

Aandachtspunt / TIP: Veilig E-mail ophalen en verzenden via uw mobiel/tablet/laptop?

Indien u e-mail ophaalt via uw mobiel/tablet/laptop kan dit ook een groot veiligheidslek zijn indien u dit niet via HTTPS (beveiligd) doet.
Uw e-mails kunnen gelezen worden door derden en tevens kunnen zij de inlogcodes van uw e-mail eenvoudig bemachtigen.

De meeste providers hebben wel mogelijkheden voor het veilig ophalen en verzenden van e-mail.
Controleer in uw e-mailprogramma of u via SSL (HTTPS) de e-mail ophaalt en verzend.

Heeft u de e-mailadressen/website via ons lopen kan dit uiteraard ook:
U haalt de e-mail dan op via **POP3.OnlineWebart.nl** poort 995 (vaak het SSL vinkje in het e-mailprogramma)
U verstuurd de e-mail dan op via **SMTP.OnlineWebart.nl** poort 465 (vaak het SSL vinkje in het e-mailprogramma)

Mochten er nog vragen zijn naar aanleiding van bovenstaande verneem ik dat graag

Met vriendelijke groet,

Maarten Heuvel
Online Software - Online Webart

	Online Groep
✉	Maarten@OnlineGroep.nl
🌍	http://www.onlinegroep.nl
	http://www.assurantiepakket.nl
☎	024-3716959
in	LinkedIn
	Postadres
✉	Postbus 6750
	6503 GG NIJMEGEN