

Download en installeer altijd updates

Inleiding

Vandaag de dag worden de meeste computerprogramma's gemaakt voor communicatie via het internet. Dat is mooi en een groot voordeel. Maar het zorgt er tevens ook voor dat zij kwetsbaar zijn voor aanvallen van buitenaf. Hackers ontdekken constant nieuwe manieren om door de verdediging van uw besturingssysteem en andere populaire softwareprogramma's heen te dringen. Softwareleveranciers reageren hierop met zgn. 'patches' (= updates!), die de pas ontdekte beveiligingsgaten dichtten. Om te zorgen dat u beschermd blijft, is het heel verstandig deze updates, zodra ze beschikbaar zijn, te downloaden en te installeren!

Internetdieven azen op onbeschermd pc's

Hackers doorzoeken het internet op pc's met kwetsbare punten in de software. Wanneer zij een manier vinden om binnen te komen, laten zij Trojaanse paarden, wormen en virussen los. Deze kunnen programmaatjes bevatten die toetsaanslagen volgen en identiteitsgegevens stelen, of programma's die hackers in staat stellen om uw computer op afstand over te nemen en/of te manipuleren.

Wat is een update?

Wanneer softwareleveranciers een nieuw beveiligingsgat ontdekken, wordt snel een update ontwikkeld en gedistribueerd om dit gat te dichtten. Updates kunnen ook worden gebruikt voor het upgraden, het repareren van een softwarefout of het toevoegen van een nieuw hardwarestuurprogramma. Veelal kunt u een update boven op een bestaand programma installeren, zonder dat u het oorspronkelijke programma opnieuw hoeft te deïnstalleren. De meeste updates zijn gratis. In bepaalde gevallen krijgen alleen geregistreerde gebruikers de updates. Het is ook mogelijk dat een update slechts beschikbaar is in een versie-upgrade, waardoor gebruikers verplicht zijn om de nieuwe versie te kopen (vaak tegen een gereduceerd tarief!).

Updates zijn bijv. nodig voor:

* Het besturingssystemen Windows 10;

* **Internettoepassingen** (Adobe Acrobat Reader DC, Adobe Digital Editions, Google Chrome, Microsoft Edge, enz.);

* **Beveiligings-, onderhouds en optimaliseringssoftware** (Genie Timeline, IObit Advanced SystemCare, IObit Driver Booster, IObit Smart Defrag, Macrium Reflect Home Free, Norton 360, Revo Uninstaller Pro, enz.);

* **Toepassingssoftware** (Adobe Photoshop Elements, MS Office Pro Plus, Roxio Creator NXT, VLC Media Player, enz.).

Hoe u kunt zorgen dat u beschermd blijft?

U kunt als volgt aan de benodigde updates komen: Leveranciers van de meeste populaire internettoepassingen zullen u bij het openen van hun programma laten weten dat er een beveiligingspatch of -update beschikbaar is. Als een betrouwbare leverancier vraagt of u de update wilt downloaden en installeren, klikt u op OK en volgt verder de aanwijzingen zoals die op uw scherm worden weergegeven. Uw Windows-besturingssysteem is mogelijk zo ingesteld dat updates automatisch worden ontvangen op het moment dat zij beschikbaar zijn. Voor andere toepassingen kunt u het beste regelmatig de website van de leverancier bezoeken om te zien of er updates zijn.

Totdat er hulp arriveert

Goede beveiligingssoftware kan uw pc en belangrijke bestanden tegen indringers beschermen, zelfs nog voordat een beveiligingsgat is gedicht. Een programma als bijvoorbeeld Norton 360 kijkt naar verdacht gedrag, dat op een inbraak zou kunnen duiden en blokkeert op voorhand pogingen om uw gegevens te stelen of uw pc te kapen.

Conclusie

Om te zorgen dat uw pc veilig is, dient u uw computer te voorzien van goede beveiligings-, onderhouds- en optimaliseringssoftware + uw besturingssysteem, internettoepassingen en andere softwareprogramma's altijd bijgewerkt te houden met de nieuwste updates.

© G. Ellens Computerhulp: December 2020