Cyber Weerbaarheidscentrum Greenport

Installeer updates tegen beveiligingslekken

Fabrikanten brengen updates uit voor hun software om nieuwe functionaliteiten toe te voegen, maar ook om fouten op te lossen en beveiligingslekken te dichten. Dat laatste is heel belangrijk. Het updaten van software kan je behoeden voor grote schade door een cyberaanval met gijzelsoftware. Lees daarom verder wat je kunt updaten en doe de test of automatisch updaten van je bedrijfssoftware verstandig is.

Weten of het voor jouw bedrijf verstandig is om je software automatisch te updaten tegen beveiligingslekken? Doe de test hier.

Een ondernemer heeft binnen zijn bedrijf al snel veel apparaten waarop software geïnstalleerd is. Voor al deze verschillende soorten software kunnen beveiligingsupdates beschikbaar zijn. Om een beter beeld te krijgen wat je op welk apparaat kunt updaten, vind je hieronder een overzicht van veel voorkomende apparaten binnen een bedrijf.

Wat kun je allemaal updaten?

Computers en Laptops

De meeste bedrijven hebben meerdere computers en laptops. En sommige bedrijven hebben ook een server op de kantoorlocatie. Elk apparaat heeft verschillende onderdelen waar updates nodig voor kunnen zijn om beveiligingslekken te voorkomen.

Besturingssysteem

De bekendste software updates voor computers en laptops zijn de updates voor het besturingssysteem. Bijvoorbeeld de updates die Microsoft voor Windows en Apple voor MacOS beschikbaar stelt. Deze updates worden vaak automatisch gedownload en geïnstalleerd, maar het is belangrijk om af en toe te controleren of dit ook werkelijk zo is.

Applicaties

Het is belangrijk te beseffen dat de updates die je installeert voor het besturingssysteem, geen updates bevatten voor applicaties die op het apparaat draaien. Denk hier bijvoorbeeld aan internet browsers, tekstverwerkers, foto bewerkers of software die PDF bestanden kan lezen. Juist op dit soort standaardapplicaties kan een beveiligingslek gemakkelijk tot misbruik leiden. Een tijdige update van de applicatie voorkomt dit. Ga daarom na welke applicaties zijn geïnstalleerd en probeer waar mogelijk automatisch updaten in te schakelen. Er bestaan tools die het mogelijk maken om veel van deze applicaties (automatisch) te updaten.

BIOS

Computers en laptops hebben onderliggende software nodig die de verschillende hardware op een lager niveau aanstuurt. Bijvoorbeeld de werking van een toetsenbord of muis. Dit soort software wordt ook wel “firmware” genoemd. De laatste jaren zijn veel kwetsbaarheden ontdekt in bijvoorbeeld processoren. Deze kwetsbaarheden kunnen vaak alleen worden opgelost door updates in de zogenaamde BIOS Firmware van een

laptop of computer en kunnen niet automatisch worden geïnstalleerd. Op de website van de fabrikant van je computer of laptop vind je deze updates met de bijbehorende installatie instructies.

Update-/patchbeleid

Het is over het algemeen zinvol voor het MKB om een update-/patchbeleid op te stellen. Hierin staan alle stappen die nodig zijn om apparaten van updates en patches te voorzien op het moment dat deze beschikbaar zijn. Gebruik het handige template in Word om snel een eigen beleid op te stellen, te vinden hier.

Netwerk

Binnen een bedrijfsnetwerk zijn vaak meerdere netwerkapparaten te vinden. Onderstaande apparaten zijn erg belangrijk om te updaten omdat deze vaak verbinding van en naar buiten mogelijk maken:

- Firewall;
- Router;
- Modem;
- Access points (draadloos netwerk).

Deze apparaten kunnen soms ook een samengesteld apparaat vormen. Updaten is bij deze samengestelde apparaten eenvoudiger omdat je alle apparaten in een keer kan updaten. Helaas is het nog niet vanzelfsprekend dat de updates automatische worden geïnstalleerd. Op de website van de fabrikant van het apparaat vind je de beschikbare updates en instructies hoe je deze installeert. Vaak wordt bij dit soort apparaten gesproken over 'firmware' in plaats van software.

Smartphones

Updates voor smartphones draaien vaak om de nieuwe functionaliteiten. Maar ook smartphones krijgen steeds meer beveiligingsupdates. Ook hier draait het om veiligheid op meerdere onderdelen van een smartphone.

Besturingssysteem

Android en iOS zijn de meest voorkomende besturingssystemen van mobiele telefoons. Een smartphone heeft veel verschillende functionaliteiten en kan dus op veel plekken een beveiligingslek krijgen. Met grote regelmaat worden daarom updates klaargezet. Bij veel smartphones kun je deze updates automatisch laten uitvoeren, check daarvoor even de instellingen.

Let op: Als je een oudere smartphone hebt, kan het zijn dat je het idee hebt dat je helemaal up-to-date bent. Het updaten van nieuwe besturingssoftware kan gestopt zijn omdat je smartphone zijn “end of life” datum heeft bereikt. Je smartphone kan dan kwetsbaar voor beveiligingslekken zijn en je zou een vervanging in overweging moeten nemen.

Applicaties

Smartphones bieden meestal een “winkel” aan waarmee applicaties kunnen worden geïnstalleerd. Houd in de gaten of deze winkel aangeeft of geïnstalleerde applicaties updates bevatten en zorg dat je deze installeert.

IoT apparaten

Het landschap van apparaten wat verbonden kan worden met een netwerk en het internet, wordt ook wel IoT (Internet of Things) genoemd. Veel IoT apparatuur wordt verkocht aan de consument, maar ook bedrijven zetten deze apparaten steeds vaker in. Denk bijvoorbeeld aan een “slimme TV” als presentatiescherm of “slimme lampen” voor de kantoorverlichting. Meer informatie over het updaten van dit soort apparaten, kun je vinden bij doejeupdates.nl.

Printers en Scanners

Printers en scanners blijven onmisbaar voor de meeste ondernemers. Een printer krijgt vaak veel gevoelige informatie toegezonden. Vaak zijn we hier ons niet bewust van. Beveiligingsupdates voor dergelijke apparaten zorgen voor het veilig houden van de communicatie die nodig is voor de print- en scanopdrachten. Moderne scanners en printers hebben vaak de mogelijkheid om automatisch updates te installeren. Omdat dit soort apparaten vaak een lange levensduur hebben, zijn er nog veel printers en scanners dit niet kunnen. Kijk op de website van de fabrikant voor de nodige updates en bijbehorende instructies.

Dit document is gebaseerd op het document ‘Installeer updates tegen beveiligingslekken’ van het Digital Trust Center. Het originele document is te vinden via https://www.digitaltrustcenter.nl/updates