

Patching (kwetsbaarheid software)



Wat is het?

- Patchen is het verhelpen van fouten in software door een nieuwe versie van (een deel van) de software te installeren die de fouten herstelt.
- Fouten in software kunnen het mogelijk maken om ongewenste acties uit te voeren, bijvoorbeeld om een systeem te hacken.
- Elke verandering van software moet gepland uitgevoerd worden, waaronder het testen.
- Het uitvoeren van een patch in bedrijven is meestal niet automatisch om onverwachte effecten te voorkomen.
- Het besluiten om te patchen hangt af van vele factoren, waaronder de impact op bedrijfsprocessen, (cyber)risico en kosten.



- **Belang voor Nederland** Om de digitale middelen te kunnen vertrouwen, moet een producent steeds op tijd fouten herstellen.
- Voor de levensduur van een product is softwareondersteuning cruciaal. De ondersteuning van de software is net zo belangrijk voor het gebruik, als het fysieke apparaat zelf.
- Patching is essentieel om de veilige & duurzame digitalisering van Nederland te realiseren.

Gevolgen bij misbruik

- Als software niet gepatcht kan worden, blijft alleen de keuze over om hackbaar te zijn of de software uit te zetten.
- Ook een software-patch kan misbruikt worden om schadelijke software te installeren. Als een leverancier gehackt is, kan een patch juist een risico introduceren.
- Ongepatchte kwetsbaarheden kunnen ervoor zorgen dat diensten uitgezet worden, bijvoorbeeld thuiswerkvoorzieningen.
- Als er geen patches meer worden verzorgd, kunnen apparaten eerder vervangen worden wat leidt tot onnodige verspilling.





Is misbruik al eens voorgekomen?

Ja, er zijn twee typen aanvallen via patches die wereldwijd (waaronder in Nederland) grote schade hebben veroorzaakt:

- Aanvallen die via een malafide patch zijn uitgevoerd; twee bekende gevallen waar zo'n aanval is uitgevoerd: Solar Winds (VS) en MEDoc (Ukraine);
- Aanvallen via het niet snel genoeg installeren van een patch: bijvoorbeeld de Citrix kwetsbaarheid in januari 2020 en de Microsoft Exchange kwetsbaarheid in april 2021.



Cybercrime specifieke relevante nationale wetgeving of andere richtlijnen

- Voor de overheid: de BIO
- Voor Aanbieders van Essentiele Diensten: de Wbni



What is patching?

- https://youtu.be/OJa0WsB_FJk?t=17

