17 mrt 2021 -13:30

400 Belgische computersystemen geïnfiltreerd na kwetsbare Microsoft Exchange server

De gevolgen van de kwetsbaarheden in Microsoft Exchange server voor Belgische organisaties en bedrijven worden steeds duidelijker. Afgelopen week waarschuwden wij al voor deze kwetsbaarheid. Uit de lijsten met kwetsbare servers konden wij meer dan 400 systemen detecteren waarbij een vorm van intrusie gebeurd is. Dit wil zeggen dat kwaadwilligen binnen gedrongen zijn in deze systemen en daar nu wachten om toe te slaan. We vrezen dan ook dat sommige organisaties en bedrijven de komende dagen en weken het slachtoffer worden van ransomware of dat er data gestolen zal worden.

Veel kwetsbare servers kregen intussen een update, maar meer dan 1000 systemen zijn nog steeds kwetsbaar. Bedrijven en organisaties die de updates wel uitvoerden, moeten ook op hun hoede blijven en hun systemen blijven monitoren. Er kunnen namelijk nog sporen achtergelaten zijn in de periode tussen de intrusie en de updates.

Het Centrum voor Cybersecurity België contacteert organisaties en bedrijven die geïnfecteerd zijn of slachtoffer van de intrusie waarvan contactgegevens beschikbaar zijn.

Wat valt er te vrezen?

Cybercriminelen installeren zogenaamde *web shells*, waardoor ze vanop afstand toegang en controle hebben via een online server. Zo kunnen ze als het ware een communicatielijn openhouden om later een aanval te lanceren. In de lijsten die wij onderzochten, vonden we minstens 400 servers waarbij een *web shell* geïnstalleerd is. In andere gevallen zou het kunnen dat hackers naast de bewuste *web shells* andere malware hebben geïnstalleerd om op een later ogenblik aan te vallen, bijvoorbeeld met een ransomware.

Wat moeten bedrijven en organisaties doen?

CERT.be, de operationele dienst van het CCB, publiceerde een advies (laatste versie 16/03)

Bedrijven en organisaties die Exchange Online gebruiken met een hybride setup of een On-Premises Exchange server voor administratieve toepassingen, moeten onmiddellijk de volgende acties uitvoeren:

- De systemen updaten
- Web shells verwijderen
- Controleren wat met de *web shell* gebeurd is
- Verdachte handelingen opsporen

De Microsoft Exchange online dienst is niet getroffen.

Bedrijven en organisaties die moeilijkheden ondervinden bij deze stappen raden wij aan om een ICT partner of externe expert in te schakelen om deze acties uit te voeren.

Meer info:

- Het volledige advies van CERT.be (geactualiseerd op 16/3)

- Het persbericht van het CCB (geactualiseerd op 16/3)
- Gebruikers met minder ervaring kunnen deze handleiding van Microsoft gebruiken. One-Click Microsoft Exchange On-Premises Mitigation Tool
- Extensive Incident Response guide (Updated by Microsoft on 16 March 2021)

Centrum voor Cyber Security België
Wetstraat 16
1000 Brussel
België
http://www.ccb.belgium.be

Andries Bomans
Communicatieverantwoordelijke
+32 471 66 00 06
andries.bomans@ccb.belgium.be

Katrien - Eggers
Communicatieverantwoordelijke
+32 485 76 53 36
katrien.eggers@cert.be