Computest

Third party mededeling

Vertrouwelijk

AFAS Software B.V.

DotNL IT Infrastructuur

26 maart 2025

Versie 1.1

Abdul Dbis, Ramin Töpfer

1. Introductie

Hierbij verstrekt Computest, op verzoek van AFAS Software B.V., een Third Party Mededeling (TPM). Deze TPM betreft het security assessment dat Computest in februari 2025, op verzoek van AFAS Software B.V., heeft uitgevoerd op de DotNL IT-infrastructuur.

AFAS heeft sinds kort nieuwe kantoorpanden ingericht die verhuurd kunnen worden aan hun partners. Deze kantoorpanden bieden innovatieve werkruimtes voor bedrijven die willen samenwerken en inspireren in een dynamische omgeving. Verschillende kantoorruimtes zijn beschikbaar, van flexplekken tot grote autonome units, voor bedrijven van elke omvang.

Het netwerk van deze kantoorpanden staat los van het hoofdnetwerk van het AFAS clubhuis. Dit netwerk is ingericht op basis van Extreme Networks en Palo Alto apparatuur en maakt net zoals het hoofdnetwerk gebruik van VRFs voor netwerksegmentatie. Dit netwerk bevat verschillende audiovisuele apparatuur, cameras en overige apparatuur ter ondersteuning van werkzaamheden in de kantoorpanden.

AFAS wil graag weten wat het beveiligingsniveau van dit interne netwerk is en welke potentiële kwetsbaarheden een aanvaller met toegang tot het interne netwerk (en de verschillende netwerksegmenten) zou kunnen ontdekken.

2. Aanpak en Scope

2.1. Aanpak

Computest hanteert een werkwijze die erop is gericht om de risico's en testdoelen zo goed mogelijk te doorgronden en te beantwoorden. Voor dit security assessment was, in overleg met de opdrachtgever, gekozen voor de onderstaande aanpak.

> Een IT infrastructuur assessment op het interne IT-netwerk. Het doel hiervan was om te bepalen of een reguliere gebruiker kwetsbaarheden kan misbruiken om toegang te verkrijgen tot gevoelige systemen.

2.2. Testonderdelen

2.2.1. IT infrastructure assessment

Het IT infrastructure assessment is een totaaloplossing waarbij, op basis van de IT-inrichting van de organisatie, alle relevante onderdelen zijn onderworpen aan een security test.

Deze security test heeft het volgende duidelijk gemaakt:

> Inzicht in de algehele beveiliging van het interne netwerk;
> Een goede indicatie of gevoelige informatie inzichtelijk is voor personen die hier geen toegang toe zouden mogen hebben;
> Bevestiging of de huidige securitymaatregelen voldoende zijn om weerstand te bieden tegen actuele cyberdreigingen, zoals ransomware;
> Duidelijkheid over hoe securityprocessen en -beleid worden gehanteerd en opgevolgd;
> Advies over hoe gevoelige informatie en systemen beter beschermd kunnen worden en handvatten om het securitybeleid naar een hoger niveau te tillen.

Op basis van de IT-inrichting en zorgen van AFAS konden testvormen worden toegevoegd of weggelaten. In overleg met AFAS is gekozen voor de volgende testvorm:

> **Intern assessment**
  > Het onderzoeken van interne systemen en diensten, WiFi-netwerken en gebruikersrechten.

>> Intern assessment

Het intern assessment heeft zich gericht op het identificeren van kwetsbaarheden waarmee toegang tot het interne netwerk kan worden verkregen, alsmede waarmee op het interne netwerk toegang kan worden verkregen tot gevoelige informatie. Tijdens dit assessment waren de volgende onderdelen onderzocht op kwetsbaarheden:

> Alle mogelijkheden om te verbinden met het interne netwerk (bedraad, draadloos, VPN);
> Mogelijkheden om via een zwak beveiligd WiFi-netwerk of een WiFi-netwerk bedoeld voor gastengebruik toegang te krijgen tot het interne netwerk en/of gevoelige informatie;
> De netwerkinrichting van het interne netwerk en hoe hierin gevoelige systemen zijn geïsoleerd;
> Systemen/diensten die beschikbaar zijn op het interne netwerk (servers, applicaties, netwerkapparatuur, printers, etc.);
> Mogelijkheden om gevoelige informatie in te zien zonder account, alsmede afgeschermde informatie die inzichtelijk is voor een medewerkers account met beperkte rechten.
> Onderzoek naar mogelijkheden tot netwerkaanvallen, bijvoorbeeld LLMNR poisoning, het ontbreken van signing voor SMB/LDAP, etc.

Netwerktoegang binnen het pand

Wanneer er zich binnen een vestiging van de organisatie netwerkaansluitingen bevinden, dan kan een kwaadwillende deze mogelijk gebruiken om direct toegang te krijgen tot het interne netwerk. Tijdens dit onderzoek is onderzocht of het mogelijk is om een netwerkaansluiting in het pand te gebruiken om toegang te krijgen tot het interne netwerk. Hierbij is ook de effectiviteit van mogelijk aanwezige beveiligingsmaatregelen getoetst.

Netwerktoegang via draadloze netwerken
De securityspecialist heeft de veiligheid van alle aanwezige WiFi-netwerken van de organisatie onderzocht. Hierbij is getoetst op:

> Mogelijke zwakheden in de standaard beveiligingsinstellingen van WiFi-netwerken;
> Mogelijke zwakheden in gebruikte netwerkapparatuur (access points, routers);
> Zwakheden in de toegangscontrole van het WiFi-netwerk, bijvoorbeeld het gebruik van een voorspelbaar wachtwoord;
> Toegang tot interne systemen en applicaties vanaf een gasten WiFi-netwerk.

Kwetsbaarheden in interne systemen en diensten
De securityspecialist heeft een security assessment uitgevoerd op aangetroffen systemen op het interne netwerk, waarbij is gezocht naar kwetsbaarheden die een aanvaller zou kunnen misbruiken. De focus lag op het identificeren van zwak beveiligde systemen op het interne netwerk, zoals slecht beveiligde servers, werkstations, netwerkapparatuur, IoT-apparaten en printers.
Hierbij zijn poortscans en kwetsbaarhedenscans uitgevoerd, waarna de securityspecialist naar eigen inzicht dieper is ingedoken op de werking van de aanwezige diensten. Een dergelijk onderzoek richt zich op het identificeren van zwakke plekken in de interne systemen en diensten en geeft handvatten om deze kwetsbaarheden structureel op te lossen.

Toegang tot gevoelige interne informatie
Dit onderzoek heeft zich gericht op wat een kwaadwillende zonder medewerkers account kan doen om gevoelige informatie in te zien waar hij/zij niet toe is gemachtigd. De securityspecialist heeft tijdens dit onderzoek het volgende in kaart gebracht:

> Welke informatie onbedoeld inzichtelijk is;
> Of er zwakheden zitten in het authenticatie- en wachtwoordbeleid van de organisatie.

Onderdelen die hierbij extra aandacht hebben gekregen zijn gedeelde netwerkschijven, gedeelde interne applicaties en intranet-functionaliteiten.

2.3. Scope

Computest heeft de volgende tests uitgevoerd:

IT Infrastructuur Assessment	
Type test	IT infrastructure assessment
Checklists	> Computest Office Automation Checklist v1.0
Domeinscope	> Geen Active Directory aanwezig
IP-scope	De interne IT-omgeving van DotNL.

2.4. Methodiek

De tests binnen een securityonderzoek zijn handmatig uitgevoerd, eventueel ondersteund door enkele tools. Computest is van mening dat hiermee betere testresultaten worden behaald, omdat testcases hierbij direct kunnen worden aangepast op de situatie. In het geval dat er automatische tools worden gebruikt zal Computest de bevindingen altijd handmatig verifiëren, om hiermee de kans op false positives te minimaliseren.

2.5. CCV-certificering

Deze test is uitgevoerd onder het keurmerk 'Cyber Security Pen Test'. Dit keurmerk, ontwikkeld door het Centrum voor Criminaliteitspreventie en Veiligheid (CCV), certificeert de kwaliteit van pentests die worden uitgevoerd door Computest. Het keurmerk verwijst naar de kwaliteit van de uitgevoerde pentest, en niet de kwaliteit van de geteste applicatie of omgeving. Meer informatie over het keurmerk is te vinden op https://hetccv.nl/keurmerken/cybersecurity/pentest/.

2.6. Kwetsbaarheidsscores

De aangetroffen kwetsbaarheden worden vervolgens door Computest voorzien van een kwetsbaarheidsscore. Hiervoor wordt gebruikgemaakt van het Common Vulnerability Scoring System (CVSS), versie 4.0. Meer informatie over dit scoresysteem is te vinden op https://www.first.org/cvss/. Iedere kwetsbaarheid wordt beoordeeld met een numerieke score tussen 0 en 10, waarbij een score van 10 de meest ernstige technische impact aangeeft.

3. Samenvatting resultaten

Computest heeft in februari 2025 een security assessment uitgevoerd op de IT-omgeving van DotNL, in opdracht van AFAS Software B.V. Het doel van deze test was om te bepalen in hoeverre de infrastructuur kwetsbaar is voor aanvallers met toegang tot het netwerk.

Uit het onderzoek blijkt dat het netwerksegment waar de partners van AFAS op aangesloten zijn (het DotNL-netwerk) goed beschermd is. Er zijn geen kwetsbaarheden gevonden in dit segment. Binnen het administratieve netwerk zijn enkele verbeterpunten geïdentificeerd. Deze punten worden proactief opgepakt door AFAS om de beveiliging verder te versterken.

Daarnaast is onderzocht of het netwerk van DotNL goed gescheiden is van het AFAS Clubhuis-netwerk. Uit de analyse blijkt dat deze segmentatie goed is doorgevoerd en dat beide netwerken strikt van elkaar gescheiden opereren.

Over het algemeen concludeert Computest dat de beveiliging van de DotNL IT-omgeving goed is en dat er geen risico's zijn waargenomen binnen dit netwerksegment.