Bijlage 1.2 Sjabloon Auditrapport

Datum
Auteur

Opdrachtgever

Securityofficer AmeRijck vakantiepark

Managementsamenvatting

In deze audit zal ik samenvatten wat de gevonden zwakheden zijn en op basis hiervan adviseren wat er verbeterd kan worden betreft beveiliging in het systeem.

Zwakheid 1 : De windows defender firewall is uitgeschakeld voor Domain profile / Private Profile & Public Profile. Inkomend verkeer heeft toegang tot alle poorten en je riskeert een grote kans op virussen en malware in jou systeem.

Advies: Schakel de firewall in! Een firewall kan het verkeer dat binnenkomt of vertrekt van een netwerk of computer beheren en filteren op basis van regels die zijn ingesteld door de gebruiker. Hierdoor kan ongeautoriseerde toegang worden geblokkeerd en verminder je de kans op malware.

Zwakheid 2: De computer loopt achter op basis van de nieuwste windows updates. In meeste gevallen bevatten deze updates beveiliging updates die een rol spelen voor jou windows applicaties, software en operating system om kwetsbaarheden te voorkomen / stabiliteit te behouden.

Advies: Overweeg het om automatisch-updates aan te zetten. Via een beleid regel kun je een tijd instellen wanneer en hoelaat updates worden geinstalleerd om latency te verminderen tijdens gebruik. Je systeem of computer blijft nu stabiel en blijft altijd up-to-date.

Zwakheid 3: Virus & Threat protection is uitgeschakeld. Hierdoor is jou systeem niet bewust dat er malicious data in het systeem is geïnfiltreerd. Denk maar aan virussen en malware dat zich kan verstoppen in jou systeem of in kleinere bestanden. Je krijgt geen melding en blijft kwetsbaar voor virussen en wormen.

Advies: Schakel Virus & threat protection in zodat je systeem dreigingen kan detecteren en dat malicious data in quarantaine wordt gezet. Zo verminder je de kans op virussen en malware! Vooral keyloggers of trojan horses & ransomware.

Zwakheid 4: Firewall & Network protection is uitgeschakeld. De firewall speelt een belangrijke rol als first layer defense voor binnenkomend en uitgaand verkeer. Omdat dit is uitgeschakeld is jou computer en netwerk kwetsbaar voor dreigingen en corruptie. Als voorbeeld ben je een makkelijk doelwit voor ransomware.

Advies: Schakel Firewall & Network protection in om je computer en netwerk veilig te houden en verminder de kans op aanvallen vanaf buiten af. Virussen, wormen, ransomware & trojans.

Zwakheid 5: App & browser control staat op waarschuwen, dit is geen cruciaal zwakheid maar als je per ‘’ongeluk’’ op toestaan klikt is je pc als nog kwetsbaar voor onbekende applicaties, extensies of files vanaf het web. Ook als je het download.

Advies: Verander de instelling van warn naar ‘’Block’’ om zeker te zijn dat je beveiligd bent voor web bedreigingen.

Zwakheid 6: De poorten 139, 445, 53, 135 of terwijl TCP poorten staan open. Aanvallers vanaf buiten het netwerk kunnen een redtool gebruiken om je netwerk in te komen om bijvoorbeeld data te stelen zoals wachtwoorden, prive gegevens en toegang krijgen tot inhoudelijke data. Ook kunnen ze je overspoelen met phishing emails.

Advies: Sluit de ongebruikte poorten om je netwerk te beveiligen tegen ongewenste binnenkomend verkeer. Je kunt dit aanpassen in de firewall met een beleid regel. Je kunt dan ddos attacks en netbios attacks preventief tegen gaan.

Overzicht onderzoek

Windows Defender Firewall, domain profile – private profile – public profile is uitgeschakeld.
Manier: Ingelogd op de server en genavigeerd naar de windows systeem instellingen voor beveiliging om te checken waarom de server helemaal kwetsbaar is. Server is bloodgesteld voor binnenkomend en uitgaand verkeer.

De computer loopt achter op updates sinds [datum] en heeft geen automatische updates aan.
Manier: Ingelogd op server en genavigeerd naar windows update instellingen om te controleren wanneer de laatste update was uitgevoerd. Windows processen en applicaties zijn out-dated en lopen belangrijke beveiliging / optimalisatie updates mis.

Virus and threat protection / firewall & network protection instellingen uitgeschakeld
Manier: Ingelogd op de server en genavigeerd naar windows beveiliging instellingen om te controleren waarom de server kwetsbaar is voor virussen. De instellingen zijn uitgeschakeld.

Apps & Files controle uitgevoerd omdat de server niet beschermd was tegen dreigingen op het web.
Manier: Op de server ingelogd vervolgens genavigeerd naar windows beveiliging onder het kopje ‘’Apps & Files’’ kun je aanvinken of je web dreigingen wilt blokkeren of liever een waarschuwing hebt.

Controle openstaande poorten (TCP) Server is niet beschermd tegen aanvallen van buitenaf.
Manier: de tool nmap gebruikt om een netwerkscan te doen op ongeregistreerde IP-adressen en openstaande poorten.

Onderbouwing keuze onderzoekshulpmiddelen

Nmap tool: netwerk scan gepleegd voor ongeregistreerde IP-adressen en openstaande poorten.

Windows beveiliging instellingen op de server: standaard informatie te vinden over de firewall en andere instellingen wat te maken heeft met beveiliging.

MBSA tool: Geeft specifiekere details om afwijken in het hele systeem.

Process explorer: advanced taakbeheer om te controleren welke onbekende processen draaien op de server en of een process of applicatie corrupt is met een malware.

Total Virus: Bestanden scannen op virussen en malware.

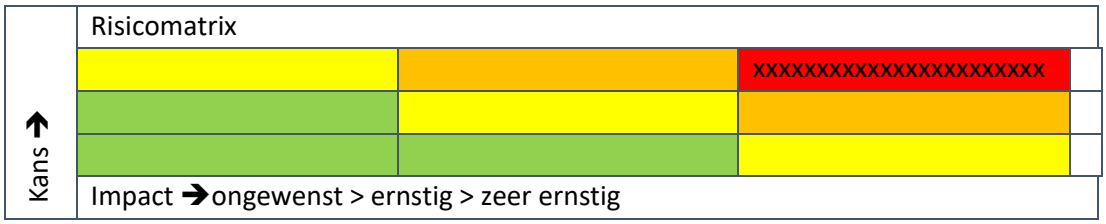
Gedetailleerde resultaten

[Voor elk gevonden issue]

1) Een beschrijving van het gevonden issue
    a. Details van het issue (bewijzen)
    b. Conclusie met impact
2) Beschrijving gevonden issue
    a. Details van het issue (bewijzen)
    b. Conclusie met impact
3) …

Conclusies

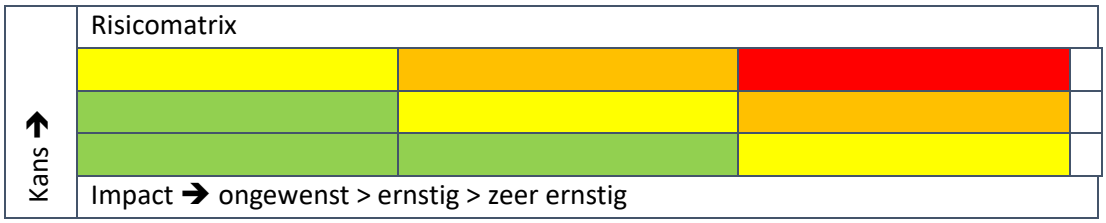
[Beschrijf jouw conclusies. Neem ook een matrix met kans en impact op van de gevonden resultaten. Nummer de resultaten en zet ze in het schema.]



Zwakheid 1: De windows defender firewall is uitgeschakeld voor Domain profile / Private Profile & Public Profile.

[printscreen bewijs van afwijking]

Kans: De kans is groot omdat het een vaak voorkomend probleem is.
Impact: ernstig, je server is heel kwetsbaar voor dreigingen en moet zo snel mogelijk als hoogste prioriteit behandeld worden.



Zwakheid 2: De computer loopt achter op basis van de nieuwste windows updates.

[printscreen bewijs]

Kans: De kans is hoog omdat er steeds nieuwe kwetsbaarheden worden ontdekt.
impact: hoog omdat er meer kwetsbaarheden komen in verouderde software.

Advies

[Geef adviezen op basis van jouw conclusies om tot een betere balans te komen voor de organisatie.]

[NB Gebruik gerust het internet, maar vermeld wel een gevonden bron en beschrijf altijd de gevonden informatie in eigen woorden.]

Trek een conclusie van alles bij elkaar.