[Gisteren 16:44] Adam Redjimi

Na gebruik van Sysinternals is er een scan gekomen. Dit heb ik gedaan met de filter VirusTotal. Er is eerder aangegeven dat de devices bevuilt zijn geraakt met een virus.  
Nu heb ik een computer van de medewerker genomen om te scannen en daaruit blijkt dat er een paar virussen gevonden zijn.

Dit gaat om een trojan virus en spyware.

[Gisteren 16:49] Adam Redjimi

De afwijkingen die ik heb gevonden bij gebruik van MBSA tool  
Afwijking 1: De automatische updates is niet geconfigureerd. (Uitleg)

Afwijking 2: 4 van de 5 accounts hebben geen expiring wachtwoord. ( Uitleg)  
ETC.

[Gisteren 16:52] Adam Redjimi

Na gebruik van NMAP zijn dit de poorten die open staan en de poorten die direct gesloten moeten worden  
Poortnummer 135  
Poortnummer 445 ( voorbeeld is gwn veilig)

Poort 135 is een DCOM service en dat zorgt ervoor dat ransomware aanvallen naar binnen kunnen komen  
Poort 445 ( file en printer sharing voor een publiekelijke PC wat alleen goed is voor een persoonlijke)

[Gisteren 17:05] Adam Redjimi

1. je text bij sysinternal is priam maar probeer het te vermelden als duidelijk onderdeel zoals:  
'na gebruik van Sysinternal zijnv lees hieronder de processen die niet gekoppeld konden worden aan een filter'

Na gebruik van Sysinternals is er een scan gekomen. Dit heb ik gedaan met de filter VirusTotal. Er is eerder aangegeven dat de devices bevuilt zijn geraakt met een virus.  
Nu heb ik een computer van de medewerker genomen om te scannen en daaruit blijkt dat er een paar virussen gevonden zijn.

Dit gaat om een trojan virus en spyware.

2. MBSA, je hebt echt veel meer afwijkingen lees maar goed.  
je dient ook hier als volgt te onderbouwen:

De afwijkingen die ik heb gevonden bij gebruik van MBSA tool  
Afwijking 1: De automatische updates is niet geconfigureerd. (Uitleg)

Afwijking 2: 4 van de 5 accounts hebben geen expiring wachtwoord. ( Uitleg)  
ETC.

3. waarom toont je scan nam NMAP waar je bevindingen te zien zijn, ook hier vermeld je als volgt:

Na gebruik van NMAP zijn dit de poorten die open staan en de poorten die direct gesloten moeten worden  
Poortnummer 135  
Poortnummer 445 ( voorbeeld is gwn veilig)

Poort 135 is een DCOM service en dat zorgt ervoor dat ransomware aanvallen naar binnen kunnen komen  
Poort 445 ( file en printer sharing voor een publiekelijke PC wat alleen goed is voor een persoonlijke)

4. riscomatrix, vermeld je netjes opgesomd de afwijkingen maar je dient daarna je keuze in de riscomatrix als volgt te vermelden:  
Onderbouwing afwijking 1 KANS: (hier je text)  
Onderbouwing afwijking 1 IMPACT: (hier je   
etc,

Afwijking 1 Trojan Virus   
Kans: Ernstig ( Kans is groot dat er problemen hierdoor onstaan, een virus kan zich zonder problemen voortnestelen in bepaalde omgevingen,netwerks wat een gevaar kan oplevernen.)  
Impact: Ernstig ( Virus kan zich uitnestelen tot een groter probleem en alles vertragen/verzieken waardoor werkzaamheden kunnen worden verhinderd. Ook kunnen er meer virussen bijkomen.  
Ransomware kan komen en dan moet er worden betaald.

Afwijking 2 Spyware  
Kans: Bovengemiddeld ( Kans is groot dat het bij iedereen geïnstalleerd wordt, kan zelfs via een link worden gedaan.)  
Impact: Bovengemiddeld ( Er kan worden meegekeken van buitenaf. Dit kan ervoor zorgen dat gegevens kunnen worden gelekt en nog veel andere dingen zoals bijvoorbeeld het achterhalen van netwerks, belangrijke documenten en andere zaken.

Afwijking 3 Poortnummer 135  
Kans: Bovengemiddeld ( Dit is de port dat als die open staat, hij open is voor ransomware en andere ongein. Dit kan heel een boel verzieken)  
Impact:Bovengemiddeld ( Ransomware, andere virussen komen binnen en dan moet er heel veel worden betaald en geregeld om het terug te krijgen.

Afwijking 4 Poortnummer 445  
Kans:Laag ( Laag dat het wordt gehackt)  
Impact:Bovengemiddeld ( Als het wordt gehackt, dan zitten mensen binnen in het systeem. Ligt er aan wie erin zit)

[Gisteren 17:09] Adam Redjimi

Details bij kans

[Gisteren 17:09] Adam Redjimi

Conclussie bij Impact