Bijlage 2.1 Sjabloon onderzoeksverslag

Datum
Auteur

Opdrachtgever

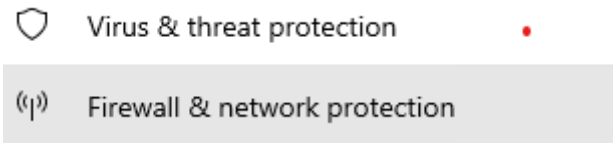
Securityofficer AmeRijck vakantiepark

Managementsamenvatting

Bij Apotheek Amerijck van het vakantiepark op Helderoog is er sprake van een securityincident. Er is een informatie lek. De acties die we hebben ondernomen zijn:
De acties die ik heb ondernomen was de wachtwoord van de database veranderd. Ook is de firewall en de virus protection aangezet zodat de computer beter beschermd is tegen de virussen en malware en als laatst heb ik de computer geupdate. De computer heeft nu ook de nieuwste software omdat het is geupdate.
Conclusie is dat de computer heel gevoelig was tegen virus aanvallen. Mijn advies is om deze acties die ik heb ondernomen om dat bij elke computer te gaan doen zodat hetnetwerk ook wat veiliger is.
[Geef hier in het kort een samenvatting voor de directie met de aanleiding, de ondernomen acties, het resultaat, een conclusie en een advies.]

Overzicht onderzoek

De firewall en virus protection is onderzocht door in de Microsoft defender te gaan kijken onder het



kopje.
De datalek in de database hebben wij onderzocht door in de server logs te gaan kijken.

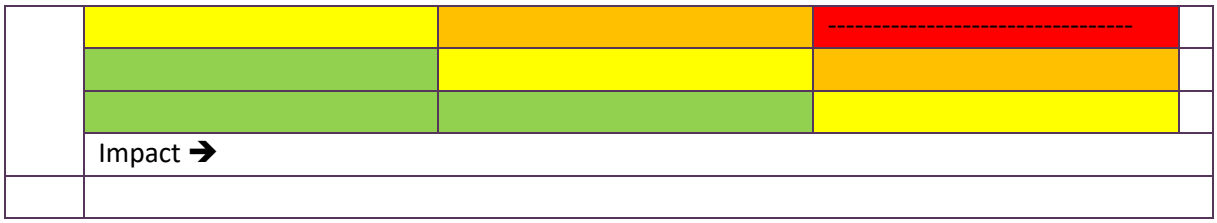
Wat is er onderzocht?

Alle controles zijn uitgevoerd op NMAP:
Hier op kijken wat er gevoelig is aan de netwerk
MBSA tool.
Hier hebben we gekeken wat er gevoelig was ana de computer
En de Windows defender hier op hebben we gezien wat er beter kon

Gevonden zwakheden

[Beschrijf de zwakheden met hun risiconiveau die mogelijk hebben bijgedragen tot het incident. Gebruik eventueel de matrix om dit overzichtelijk te rapporteren.]

✓	Risicomatrix



1ste gevonden zwakte was de virus die in de computer zat dit is heel erg gevaarlijk want hierdoor is de datalek gebeurd

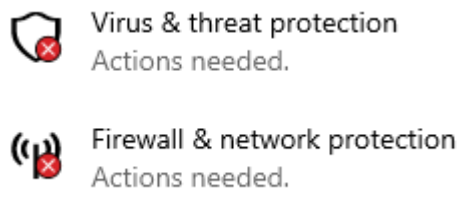
De tweede gevonden zwakte was de firewall die uitstond. Dit is heel gevaarlijk omdat inkomend en uitgaand netwerkverkeer niet bewaakt. Want wat de firewall doet is bepalen of welk verkeer wordt toegestaan of geblokkeerd op basis van een gedefinieerde set security regels.

Remote acces tool stond zelf is dat niet zo gervaarlijk als je firewall aan staat, maar omdat het wel uit stond bij deze computer is best wel gevaarlijk. Computer kunnen van buiten af verbinding gaan maken met je computer en een RAT kunnen op sturen.

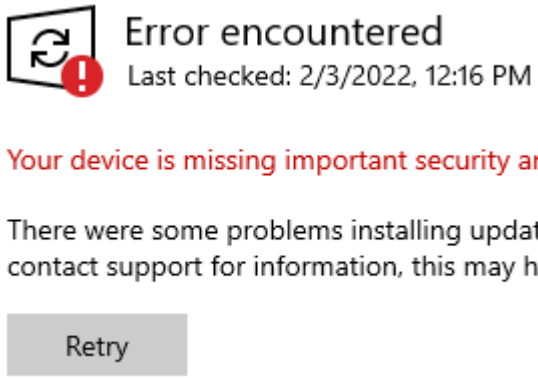
De wachtwoord van de database was: root. Dit is echt heel onveilig omdat het heek makkelijk te kraken is. Dus de database was totaal niet goed beveiligd.

De antivirus stond uit dus hier konden alle virussen en malware makkelijk in de computer door dringen en bestanden afpakken.

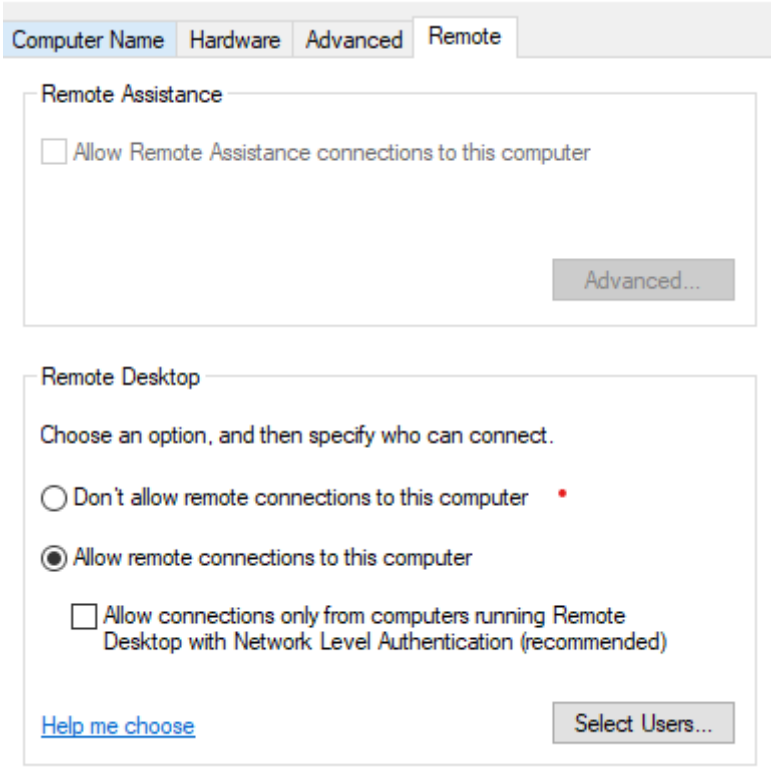
Beschrijving gevonden bewijzen van eventueel misbruik



Hier was er misbruik van gemaakt omdat je heel makkelijk in de computer kan komen



Hier was er misbruik van gemaakt omdat de computer niet voorbereid was tegen de nieuwste virussen en malware.



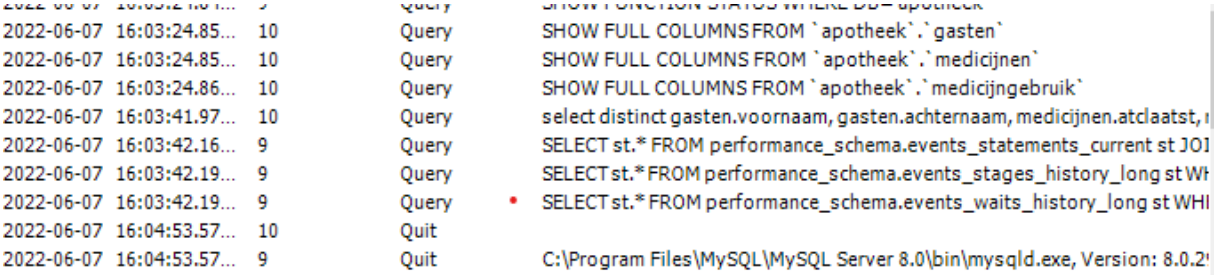
Hier is er ook misbruik van gemaakt omdat de computer van een andere computer een RAT opgestuurd kan krijgen waardoor er ene virus in uw computer komt.

Inhoud van gevonden bewijzen

Het bewijs wat ik heb gestuurd is dat de computer heel gevoelig was tegen aanvallen van buiten af ook omdat de remote acces tool aan stond terwijl dat de firewall en virus protection uitstonden.

Bericht mogelijk datalek

Er moet een melding worden gemaakt naar de meldloket omdat er gevoelige data kwijt is geraakt dat op de zwarte markt terecht kan komen.



2022-06-07	16:03:24.85...	10	Query	SHOW FULL COLUMNS FROM `apotheek`.`gasten`
2022-06-07	16:03:24.85...	10	Query	SHOW FULL COLUMNS FROM `apotheek`.`medicijnen`
2022-06-07	16:03:24.86...	10	Query	SHOW FULL COLUMNS FROM `apotheek`.`medicijngebruik`
2022-06-07	16:03:41.97...	10	Query	select distinct gasten.voornaam, gasten.achternaam, medicijnen.atclaatst,
2022-06-07	16:03:42.16...	9	Query	SELECT st.* FROM performance_schema.events_statements_current st JOI
2022-06-07	16:03:42.19...	9	Query	SELECT st.* FROM performance_schema.events_stages_history_long st WH
2022-06-07	16:03:42.19...	9	Query	SELECT st.* FROM performance_schema.events_waits_history_long st WHI
2022-06-07	16:04:53.57...	10	Quit	
2022-06-07	16:04:53.57...	9	Quit	C:\Program Files\MySQL\MySQL Server 8.0\bin\mysqld.exe, Version: 8.0.2

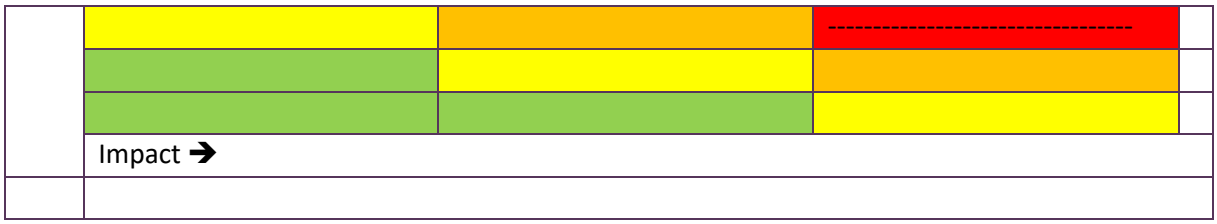
Hier heeft zich de datalek plaatst gevonden. Er zijn drie soorten gegevens gelekt:

1. Gasten
2. Medicijnen
3. Medicijnengebruik

Alle personen die hier hun medicijnen vandaan haalt is een slachtoffer van de datalek.

Conclusie

De conclusie is dat de computer slecth was beveiligd door dit:



1ste gevonden zwakte was de virus die in de computer zat dit is heel erg gevaarlijk want hierdoor is de datalek gebeurd

De tweede gevonden zwakte was de firewall die uitstond. Dit is heel gevaarlijk omdat inkomend en uitgaand netwerkverkeer niet bewaakt. Want wat de firewall doet is bepalen of welk verkeer wordt toegestaan of geblokkeerd op basis van een gedefinieerde set security regels.

Remote acces tool stond zelf is dat niet zo gervaarlijk als je firewall aan staat, maar omdat het wel uit stond bij deze computer is best wel gevaarlijk. Computer kunnen van buiten af verbinding gaan maken met je computer en een RAT kunnen op sturen.

De wachtwoord van de database was: root. Dit is echt heel onveilig omdat het heek makkelijk te kraken is. Dus de database was totaal niet goed beveiligd.

De antivirus stond uit dus hier konden alle virussen en malware makkelijk in de computer door dringen en bestanden afpakken.

[Beschrijf jouw conclusies. Neem ook een matrix met kans en impact op van de gevonden zwakheden.]

Advies

Mijn advies is om de wachtwoord te gaan veranderen van de database. Ook is mijn advies aan u om de virus protection en de firewall aan te zetten zodat uw computer stukken beter word beschermd tegen virussen en malware. En de instelling automatisch updaten aan te zetten zodat uw computer goed is beschermd tegen de laatste virussen en malware.

Communicatieadvies

Wij adviseren de organisatie om volgens de onderstaande communicatiematrix te communiceren. [Kruis aan wie welke informatie moet gaan krijgen.]

	Gevonden zwakheden	Beschrijving gevonden bewijzen	Inhoudelijk gevonden bewijzen	Aangebrachte aanpassingen	Bericht mogelijk datalek
Jouw leidinggevende	x	x	X	x	x

Securityofficer van AmeRijck	X	x	X	X	x
Directie van AmeRijck	X			X	X
Lokale media				X	X
Nationale media	X			X	X
Meldloket datalekken	X			X	X
Politie	X	X	X	X	X
De afdeling IT van AmeRijck	X	X	X	X	X
De afdeling Marketing van AmeRijck				X	X
De receptie van AmeRijck	x			x	X

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