Actie nr.	Wat is er aan de hand?	Wat is het gevaar?	Hoe hoog is het risico	Oplossing	Kosten in tijd en geld	Verandert de gebruikerservaring?	Implementator	
1	De VPN inbelverbinding heeft geen MFA.	De VPN kan gebruikt worden met credentials die verkregen zijn door een hack, phishing mail etc.	Laag	MFA implementeren op de VPN inbelverbinding.	Dit moet geconfigureerd en gecommuniceerd worden, dit kost 20 uur.	Er is een extra stap in de inlogprocedure.	Sjonnie	
2	Disable TLS1.0 en TLS1.1 support servers ADFS omgeving.	Worden wereldwijd als onveilig gezien, MITM attack, Vanaf eind januari grade will be capped naar B op adfs omgeving bij SSL-Labs.	Middel	Moet geconfigureerd worden op de servers ADFS omgeving.	20 uur	Nee	Sjonnie	
3	Examen pc's worden niet structureel gepatched omdat deze middels pxe booten naar de non windows omgeving	Het doel is alles structureel patchen. Als dit niet plaatsvindt dan heb je zwakke plekken binnen het patchbeleid.	Middel	ADR voor maandelijks patchen staat klaar. Technische oplossing voor boot naar pxe (bootfile per location)	40 uur	Nee	Raymond/Willem	
4	Desktop pc's worden niet structureel gepatched omdat dit niet ingeregeld is	Het doel is alles structureel patchen. Als dit niet plaatsvindt dan creer je zwakke plekken binnen het patchbeleid.	Middel	ADR voor maandelijks patchen staat klaar.	8 uur	Nee	Gary, Willem, Arnoud, Raymond, Nico	
5	Non microsoft Applicaties worden handmatig en niet dekkend gepatched	Het doel is alles structureel patchen. Als dit niet plaatsvindt dan creer je zwakke plekken binnen het patchbeleid.	Laag	3rd party solution, handwerk	320 uur	Meer updates	Gary	
6	Local administrator account staat aan op laptops, en het wachtwoord wordt niet regematig gewijzigd. Is ook vaak bekend bij stagiaires	Brute force hack op het wachtwoord, privilege escalation	Middel	Microsoft LAPS (Local Administrator Password Solution)	40 uur	Nee	Willem	In behandeling, ingeregeld voor laptops.
7	Oneigenlijk gebruik van de laptops, gebruik voor niet werk doeleinden	(Onbewust) Installatie van malware, root kits, hack tools	Middel	Beleidsverandering	NNB	Ja, men verliest het recht om alles te kunnen op de laptop	Bas (Beleid)	
8	Iedereen is local administrator	(Onbewust) Installatie van malware, root kits, hack tools	Middel	Beleidsverandering	NNB	Ja, men verliest het recht om alles te kunnen op de laptop	Bas (Beleid)	
9	Testomgeving wordt niet voldoende / structureel gepatched	Het doel is alles structureel patchen. Als dit niet plaatsvindt dan creer je zwakke plekken binnen het patchbeleid.	Middel	ADR op SCCM inregelen op Test	40 uur	Nee	Arnoud	
10	Vulnerabiliy caused by installed non enterprise software	Het doel is alles structureel patchen. Als dit niet plaatsvindt dan creer je zwakke plekken binnen het patchbeleid.		Alle computers naar 1809, Azure MDM Security Baseline (Intune)	100 uur	Ja, meer patches	Gary	
11	Niet alle back-up gaat ook off site	Als er toch ransomware op de storage van de back-up server komt hebben we geen back-up behalve minimale cloud back-up.	Middel/Hoog	Of cloudstorage vergroten zodat deze dekkend is of offline back-up inregelen (bijvoorbeeld tape storage).				
12	200 laptops Spo5 worden niet structureel gepatched	Het doel is alles structureel patchen. Als dit niet plaatsvindt dan heb je zwakke plekken binnen het patchbeleid.	Middel					
13	Back-up storage server staat in het domein en zelfde netwerk	Makkelijkere toegang tot de storage server voor kwaadwillenden	Middel	Storage buiten npc netwerk plaatsen				
14	Gebrek aan disaster recovery en het structurele testen hiervan							
15	Niet alle servers kunnen worden ge-update door het gebruik van legacy applicaties (Artifax en Hotel Concepts)	Servers die niet voorzien zijn van de laatste updates zijn kwetsbaarder voor aanvallen.	Middel/Hoog	Uitfaseren legacy applicaties		Er moet een andere applicatie worden aangeschaft.	TAB / Cloudbeher	
16	Verbeterde netwerk sementatie en ACL's	Sommige servers zijn bereikbaar vanaf BYOD device netwerken	Middel/Hoog	ACL's toepassen	60	Nee	Datacom	
17	Elasticsearch	Het makkelijk kunnen zoeken in de logging mbt tot beveiligingsincidenten	Laag	Combined Logging in de vorm van Elasticsearch (Project C2019008 hier voortzetten)	60	Nee	Sjonnie	
18	Disable TLS1.0 en TLS1.1 in de Fortiweb omgeving	Worden wereldwijd als onveilig gezien, MITM attack.	Middel	Moet geconfigureerd worden op de Fortiweb omgeving.	4 uur	Nee	Sjonnie	
19	Defender Advanced Threat Protection	More secure	Middel/Hoog	Afhankelijk O365 A5 license	20		Gary	
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								
32								
33								
34								
35								
36								
37								
38								
39								