CASE STORY: GO!

Over GO!

Het GO! onderwijs van de Vlaamse Gemeenschap is de Vlaamse openbare instelling voor het gemeenschapsonderwijs. Het GO! is een van de drie onderwijsnetten in Vlaanderen. Het GO! telt 1000 instellingen voor kleuter-, lager, secundair en volwassenenonderwijs en meer dan 38.000 personeelsleden. In het voltijds onderwijs bedient het GO! met 330.000 leerlingen zo'n 15 à 20% van de Vlaamse schoolbevolking.

Over SecWise

SecWise is een team van cloud security experts, toegewijd om onze klanten te helpen met cyber security en compliance in hun digitale transformatie naar een cloud en mobiele werkomgeving. Door het toenemende gebruik van cloudinfrastructuur en mobiele toepassingen wordt de te beschermen omtrek steeds groter. Onze missie is om ervoor te zorgen dat beveiliging geen belemmering vormt voor het verhogen van de productiviteit en de bijbehorende digitale transformatie, in tegendeel, dat het deze overgang op een veilige manier kan faciliteren.

GO! wint een halftijdsequivalent met nieuwe securitytoepassing van Microsoft

Anderhalf jaar geleden werd het Gemeenschapsonderwijs het slachtoffer van digitale inbraakpogingen. Met name de software voor virtuele desktops werd geviseerd. Voor ICT-manager Jan Buytaert was dat niet alleen het finale signaal om de migratie naar Microsoft Azure en Microsoft Office 365 te versnellen, het was ook de aanleiding om cyberbeveiliging wat steviger in handen te nemen. Op advies van zijn cybersecurityspecialist Secwise voegde GO! de beveiligingssuite Microsoft 365 Defender toe aan zijn migratieplannen.

Wat zijn de key take-aways?

- GO! krikt cyberbeveiliging op met Microsoft 365 Defender
- Automatische phishingcontrole op laptops spaart halve VTE uit
- Azure Sentinel monitort cyberveiligheid, deels geautomatiseerd

Welke cijfers moet jij onthouden?

- 400: mailboxen van de centrale diensten worden gescand op malware en spam
- 2: binnen twee jaar wil GO! volledig vanuit de cloud werken
- 3: toepassingen van de beveiligingssuite heeft GO! al geactiveerd

"Een strakke security is een absolute noodzaak", zegt ICT Manager Jan Buytaert, "toch deden er zich bij het begin van het kalenderjaar een aantal cyberincidenten voor. Die hadden een impact op onze werking, en overtuigden onze directie om onze kwetsbaarheden bloot te leggen en vervolgens te beveiligen. We hebben binnen het kader van een bestaand raamcontract Secwise aangesteld om een beveiligingsaudit voor ons uit te voeren."

Microsoft 365 Defender

Secwise vertaalde de audit van een twintigtal stappen naar een roadmap met een hele reeks aanbevelingen. ***"In het verleden had je voldoende met een firewall en antivirus, maar nu kun je niet langer enkel op die producten teren"***, zegt Koen Jacobs van Secwise. "Omdat het GO het eigen datacenter wil afbouwen ten voordele van de cloud – en daarbij vooral naar Microsoft-technologie overstapt, adviseerden we om hun licentie uit te breiden naar A5, waar ook de beveiligingssuite Microsoft 365 Defender in vervat zit."

Daarmee kan GO! niet alleen laptops beveiligen, maar ook zijn e-mailtoepassing vrijwaren van spam én zijn nieuwe cloudomgeving vrij van malware houden. "Vaak denkt men dat de cloud al veilig is, maar je bent nog altijd zelf verantwoordelijk voor wat er op hun -weliswaar beveiligde- platform gebeurt. Voor de beveiliging van de toepassingen die erop draaien, moet je zelf zorgen", zegt Buytaert.

Het Gemeenschapsonderwijs maakte een bewuste keuze voor Microsoft. "We zijn als IT-dienst al goede klant bij hen, onze ontwikkeling doen we ook met hun software. We werken ook met Microsoft Office 365 en Microsoft Azure. Microsoft 365 Defender kun je 100% pluggen op hun bestaande toepassingen zoals Teams en Outlook. Met een druk op de knop waarschuw je anderen voor gevaarlijke e-mails of spam. We zijn dus vooral vanuit gebruikersperspectief naar Microsoft gegaan", vertelt Jan Buytaert.

> ***Het was voor april bijna een dagtaak om phishingpogingen te analyseren. Nu houdt Defender ATP ze automatisch tegen, het scheelt ons een halve voltijdsequivalent.***
>
> *– Jan Buytaert, ICT Manager van GO!*

Virusscanner op 400 laptops houdt onder meer phishing tegen

Stap één in de nieuwe beveiligingsstrategie was de toevoeging van Microsoft Defender Advanced Threat Protection aan de Windows 10-toestellen van GO! Dat project startte net voor de coronalockdown en is tegen eind 2020 klaar. GO scant wel al de mailbox van 400 medewerkers van de centrale diensten op spam en malware, en dat wordt Buyaert al gewaar: “Het was voor april bijna een dagtaak om te bepalen of bepaalde mails al dan niet phishingpogingen waren. Nu houdt Defender ATP ze automatisch tegen, het scheelt het team een halve voltijdsequivalent.”

> ***Security kun je in grote strategieën gieten, maar Secwise gaat zeer snel concreet. Dat maakt hen ook kostenefficiënter dan anderen.***

Slimmer worden met Azure Sentinel

Om de visibiliteit in hun netwerk te verhogen en een beter inzicht te hebben in de cyberbeveiliging, activeerde Secwise ook Azure Sentinel. Dat is *security incident & event management software*, waarmee het securityteam elk cyberincident kan inkijken en aanpakken. Koen Jacobs: “Daarmee willen we de servers beter monitoren. We willen alle ‘beveiligingslogs’ van elke toepassing naar Azure Sentinel sturen, automatisch filteren en desnoods actie ondernemen. Kwaadaardige bestanden zet Sentinel automatisch in quarantaine. Er is ook een *machine learning* component die helpt om vals positieven te ontdekken.”

“We zijn een klein team maar moeten dezelfde diensten leveren als een grote IT-dienst”, vult Buytaert aan. ***“Met slimme software zoals Sentinel kun je nu veel taken automatiseren. Zo hoeven we ook geen gespecialiseerde technische opleiding te voorzien voor onze mensen.”***

In de toekomst wil GO! toestellen van op afstand beheren

Met identiteits- en toestelbeheer staan de volgende securityprojecten al in de steigers. De ICT-manager wil in eerste instantie de GO!-toestellen efficiënter beheren. “Onze huidige *device management software* werkt niet goed vanop afstand. Corona toont aan dat dat een probleem is. Met Microsoft Endpoint Manager zouden we dat beter aanpakken. Maar we denken er ook aan om *security managed services* af te nemen zodat een expert onze beveiliging mee in de gaten houdt.”

Opnieuw kijkt de ICT-manager dan in de richting van Secwise. “Zij zijn zeker niet de eerste securitypartner die hier is gepasseerd, maar mijn collega’s zijn zeer tevreden van hun transparantie, pragmatisme en concrete info. Over security kun je boeken schrijven en theoretische modellen toepassen, maar Secwise gaat zeer snel concreet. Ze behouden het totaalplaatje, maar vertalen die meteen in producten en tools. Dat maakt hen ook kostenefficiënter dan anderen. Van strategie tot concrete uitvoering werken we erg vlot samen.”