CASE STORY: FIT

Over FIT

De Vlaamse overheid riep in 2005 Flanders Investment & Trade (FIT) in het leven. Het agentschap helpt Vlaamse bedrijven om hun activiteiten in het buitenland uit te breiden en helpt buitenlandse bedrijven bij het vinden van Vlaamse leveranciers van kwaliteitsgoederen en -diensten. FIT heeft zijn hoofdkwartier in Brussel en telt 70 kantoren over de hele wereld.

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.

Secwise doet voor FIT cyberdeuren op slot

In 2015 trok Flanders Investment & Trade een IT-strategie op gang die hen stelselmatig naar de cloud zou brengen. Met een hoofdzetel in Brussel, 5 kantoren in Vlaanderen en 70 kantoren en ruim 250 medewerkers in het buitenland valt daar wat voor te zeggen. Tegelijk kwam er naast de traditionele, centrale perimeterbeveiliging ook aandacht voor decentrale cyberveiliging. Na verschillende security-audits en evaluatie van een aantal beveiligingstoepassingen koos FIT voor de beveiligingssuite van Microsoft 365 Defender. ***“Die leent zich niet alleen prima bij onze cloud-only aanpak, Microsoft scoort vandaag ook zeer goed in security benchmarks”***, zegt Team Manager IT Kurt Spitaels.

Wat zijn de key take-aways?

- FIT schakelt volledig over naar cloud
- Met de Microsoft 365 Defender suite beveiligt de organisatie zijn cloud-only aanpak
- Vandaag heeft FIT een veel beter zicht op zijn beveiliging en op mogelijke beveiligingsinbreuken

Welke cijfers moet jij onthouden?

- FIT implementeerde alle M365 Security componenten
- 400: medewerkers werken nu veilig vanuit de cloud
- 5: in vijf maanden zijn alle toestellen en cloud servers beveiligd met de nieuwe security

Onder impuls van de klassieke voordelen – flexibel, operationele kost, geen hardware meer, decentraal en van overal toegankelijk… – krijgt de reis van Flanders Investment & Trade naar de cloud almaar nieuwe bestemmingen. Vanaf 2015 verving de organisatie stapsgewijs onder meer zijn *on premise* IBM Domino omgeving voor Microsoft Azure, Microsoft Dynamics en Office 365 met onder meer Exchange en SharePoint. Daar voegde het Skype for Business met PSTN-connectiviteit aan toe, en inmiddels PSTN-telefoneert FIT met Microsoft Teams via *direct routing*. Ook daarin is voor FIT een pioniersrol weggelegd.

Voor een passende beveiliging van al die cloudtoepassingen nam FIT contact op met SecWise, een cybersecurityspecialist uit De Cronos Groep. “Microsoft beveiligt immers wel zijn centrale datacenter, maar niet zozeer de lokale omgeving van de gebruiker. We vroegen dan ook aan Secwise om te analyseren waar er mogelijke hiaten in onze securitystrategie waren. Zij deden een assessment van vijf dagen met pen- en cloudbeveiligingstests, en tekenden vervolgens een implementatie uit van drie fases over vijf maanden”, zegt Kurt Spitaels.

Migratie naar de volledige beveiligingssuite van Microsoft

Bij de overstap naar Microsoft Teams en de vernieuwing van zijn licentiecontract, bleek dat FIT al zeer dicht bij Microsofts E5-licentie aanleunde. Die omvat ook de volledige securitysuite Microsoft 365 Defender. “Die suite paste perfect bij onze decentrale en cloud-only aanpak, en vooral ook ons Microsoft-portfolio: de integratie is uiteraard veel nauwer dan wanneer je met andere leveranciers werkt. ***Daardoor blijf je aanvallers toch een aantal stappen voor.*** Als het versnipperd is zonder doorstroming van intelligentie, krijg je een vals gevoel van veiligheid”, zegt Kurt Spitaels. “Bovendien moet ik in ons kleine IT-team het aantal producten beperken. Ik kan geen 20 experts aanwerven per securitytoepassing. Microsoft dekt ten andere hoe langer hoe meer af.”

> ***De sterke integratie van Microsoft 365 Defender met andere Microsoft-toepassingen biedt een aantal aanzienlijke securityvoordelen. Als je security versnipperd is, zonder doorstroming van intelligentie, krijg je een veel minder geïntegreerd beeld en een vals gevoel van veiligheid.***
>
> *– Kurt Spitaels, Team Manager IT bij FIT.*

In een eerste fase beveiligde FIT zijn Microsoft Office 365-kantoortoepassingen. Het activeerde Office 365 Advanced Threat Protection die onder meer mails met spam en malware tegenhoudt. Tegelijk paste FIT Microsofts zero trust-model toe, met *conditional access* om de computers en gebruikers nog meer te beschermen: we vertrouwen niemand en er is een extra voorwaarde om toegang te krijgen. Die voorwaarde is dat de gebruiker multifactorauthenticatie moet gebruiken om aan te melden met een *authenticator app*. Als je aanmeldt in Brussel en twee uur later in Mogadishu, dan zullen wij hiervan een *"impossible activity"* melding krijgen. Al deze meldingen worden systematisch onderzocht en opgevolgd: controle van valse meldingen, hertstellen van wachtwoorden, blokkering van connecties, enzovoort.

> ***Als je aanmeldt in Brussel en twee uur later in Mogadishu, moeten er knipperlichten opspringen en moet je securitychecks opstarten.***

Strakke controle over FIT-toestellen

In een tweede fase nam FIT Microsoft Endpoint Manager (Intune) in gebruik, software voor toestelbeheer. “Wij beheren en configureren alle computers en telefoons van onze medewerkers wereldwijd. Computers vertrekken allemaal vanuit Brussel, telefoons worden lokaal aangeschaft. Door de *policies* te bepalen met Endpoint Manager kunnen we ervoor zorgen dat men bijvoorbeeld enkel welbepaalde, goedgekeurde apps kan gebruiken. ***En indien nodig kunnen we toestellen van op afstand leeghalen in geval van diefstal***”, zegt Kurt Spitaels. Voor een optimale cyberbescherming installeerde FIT Microsoft Defender ATP op de computers van de medewerkers, en Azure Advanced Threat Protection voor het beschermen tegen lateral movement attack technieken.

In een vierde fase ten slotte activeerde de organisatie een nieuw Azure Security design, die de public cloud omgeving beveiligt. Koen Jacobs, managing partner van Secwise: “Vaak beperken bedrijven zich tot een lift-and-shift van hun applicaties naar Azure, maar je moet ook de beveiliging aanpassen. Tijdens vrijwel elk assessment worden nog deurtjes gevonden die niet goed op slot zijn. Als aanvulling hebben we voor FIT dan ook een beveiligingsreferentiekader of ‘security governance’ uitgewerkt.”

Maak het tegenstanders zo moeilijk mogelijk

Cyberbeveiliging bij FIT is de voorbije jaren met grote stappen vooruitgegaan maar blijft een continu aandachtspunt.. ***"Vroeger bleven inbraakpogingen veel gemakkelijker onder de radar"***, geeft Kurt Spitaels toe. "Door de beveiliging te verhogen maak je het moeilijker voor de tegenstander. Niet vergeten dat we in cybergevoelige landen zitten en dat er bij ons soms ook gevoelige informatie in omloop is. Vandaag hebben we een beter zicht op al onze componenten en krijgen we sneller en meer signalen waar er potentieel malware is afgeleverd."

Dat is meteen een van de redenen waarom FIT met Cronos en SecWise in zee ging. "We vonden er de juiste profielen en ervaring. Een sluitende beveiliging vraagt de nodige investeringen maar we kunnen ons niet veroorloven om halfslachtig te werken. Security is te belangrijk. Met SecWise houden we onze securitymaturiteit op peil, en proberen we continu onze zwakheden af te dekken. Daarom hebben we ook naar hen gekeken voor de eerste screening van alerts en om maatregelen rond *shadow IT* mee uit te werken . ***Security is a journey, not a destination.***"