

Risico's van externe cyberveiligheid en vertrouwensbeheer, twee zijden van één medaille

21 december 2021, 01:00

Tatiana Galibus

De cyberveiligheidsexperts van Sirris doen interessante leerervaringen op uit de individuele coaching-sessies ter plaatse in de bedrijven. In deze blog delen we enkele van de vele praktische waarnemingen op het terrein en we geven enkele tips op basis van onze ervaring met de veiligheid van de toeleveringsketen en hoe de bedrijven daarmee omgaan.

We krijgen frequent te maken met klanten die onvoldoende kennis of ervaring hebben in het veilig interageren met derden (m.a.w. bedrijven verlenen technologieproviders vaak bestuurdersrechten in hun interne netwerken, openen poorten voor externe toegang zonder monitoring of beperkingen enz.). Dit vormt een directe bedreiging voor de kritieke activa en de bedrijfscontinuïteit.

Anderzijds coachen we geregeld digitale-technologieproviders die van klanten vragen krijgen rond het thema 'vertrouwen', zoals:

- Zijn uw activiteiten beveiligd?
- Kan ik u mijn gegevens toevertrouwen?
- Wat zijn de garanties dat uw dienst/digitaal product niet zal worden gekraakt?

We stellen vast dat de veiligheid van de toeleveringsketen een almaar belangrijker thema wordt en meer aandacht van beide partijen vereist.

U bent een outsourcer?

Telkens wanneer u toegangsrechten verleent tot digitale diensten, of het nu gaat om een app, een cloudplatform, een mobiele app, SaaS of andere, loopt u een potentieel risico. Uw interne infrastructuur, rekeningen, activa, productielijnen en gevoelige gegevens worden aan de externe dienst blootgesteld op dezelfde manier als aan uw eigen interne dienst. Maar kunt u derden wel vertrouwen? En hoe controleert u de veerkracht van een technologieprovider vóór u hem toegang tot uw netwerk verleent?

In deze realiteit vormen interacties met derden een bedreiging. Iedereen herinnert zich nog [de aanval op Solarwinds in december vorig jaar](#). De feiten:

- De aanval trof ruim 18.000 bedrijven.
- Hij was afkomstig van een cyberveiligheidsprovider (Solarwinds service) via een routine-update
- Veel bedrijven wisten niet dat ze het slachtoffer waren van de aanval omdat ze geen logs hadden.

- Zelfs het Amerikaanse ministerie van Financiën werd getroffen.

Kunnen we, met dit bewijs in handen, in 2021 blindelings vertrouwen op onze externe veiligheidsproviders? En wat moeten we praktisch gezien doen?

Onze aanbeveling? De enige manier om een vertrouwensband op te bouwen, is vragen te stellen. U kunt in zee gaan met een externe auditor (u betaalt hem en vertrouwt erop dat hij uw meest waardevolle bedrijfsmiddelen auditeert), maar tegelijk MOET u ook uw eigen bewustzijn vergroten. Lijkt dit moeilijk? Dit is precies waar Sirris en Agoria aan werken: probeer onze korte, gratis webinars over vertrouwen en veerkracht uit (u vindt ze binnenkort in onze agenda), of onze huiseigen stapsgewijze, praktijkgerichte en pragmatische masterclasses voor bouwers van digitale diensten en outsourcers. We doen er alles aan om u de beste leerervaring te bieden!

U bent een digitale-technologieprovider?

In 2021 stelden klanten u al vragen over cyberveiligheid en het zal vragen blijven regenen! Het is bewezen dat de meeste bedrijven bij het werken met digitale-technologieproviders, ongeacht de technologie, de volgende vragen van klanten krijgen:

- Bent u veilig genoeg?
- Hoe kan ik u mijn gegevens toevertrouwen?
- Aan welke normen voldoet u?
- Hebt u penetratietesten uitgevoerd?
- Wat is uw veiligheidsniveau?

Om een deal rond te krijgen, is het vaak essentieel om deze vragen te kunnen beantwoorden; vertrouwen wordt bijgevolg een prioriteit in de bedrijfscontinuïteit voor digitale-serviceproviders. Hoe gaat u tewerk? Goed nieuws voor digitale diensten: er bestaat een duidelijke oplossing, met name AppSec worden. AppSec worden betekent gewoon dat u van meet af aan de beginselen van een veilig ontwerp toepast. Deze beginselen zijn beter gekend als de [Application Security Verification Standard](#). Van daaruit bouwt u uw dienst op volgens de DevSecOps-concepten. U leest er hier alles over en u kunt ook onze masterclass over cyberveiligheid voor bouwers van digitale diensten volgen!

Het veiligheidsbewustzijn verhogen

Werken met derden impliceert vaak ook een menselijke factor en vertrouwenskwesaties. Om dergelijke vragen te kunnen beantwoorden of stellen, moet u over kennis rond veiligheid beschikken. Het klinkt misschien ingewikkeld of eng, maar in de praktijk is dit de goedkoopste en snelste manier om de veiligheid te verbeteren. Het bewustzijn verhogen is goedkoper en efficiënter dan het aankopen van complexe instrumenten en oplossingen (waarvoor nieuwe opleidingen nodig zijn). De beste manier om in cyberveiligheid te investeren is in geregelde trainingen te investeren! Hoe doet u dat op een slimme manier? Sirris en Agoria bieden een ruime waaier van mogelijkheden:

- Gratis webinars over Vertrouwen en Veerkracht (binnenkort in onze agenda)
- Masterclasses (gesubsidieerd door VLAIO; Vlaamse bedrijven betalen bijgevolg slechts 30 procent van het bedrag) met hands-on aanpak, praktische tips en stapsgewijze begeleiding:

Auteurs



Tatiana Galibus