Two sides of a coin: third-party cybersecurity risks and trust management

16 December 2021, 01:00

Tatiana Galibus

At Sirris cybersecurity experts gain interesting learning experience from individual coaching on company premises. In this blog we share with you some of the many practical observations from the field. Here are some tips based on our experience with supply chain security and how it is dealt with in the companies.

We are often confronted with customers who lack knowledge or experience of managing their third party interactions in a secure way, i.e. companies often give administrator rights to technology providers in their internal networks, open ports to the external access without monitoring and restrictions, etc. This creates a direct threat to critical assets and business continuity.

On the other hand, we often coach digital technology providers who receive questions on the topic of trust from the customers, such as the following:

- Are you secure?
- Can I trust you with my data?
- What are the guarantees that your service/digital product will not be breached?

We are constating that the topic of supply chain security becomes more and more important and requires more attention from both sides.

You are an outsourcer?

You are potentially at risk every time you give access rights to digital services, whether it is an app a cloud platform, mobile app, SaaS, etc. Your internal infrastructure, accounts, assets, production lines, sensitive data are exposed to the external service in the same way as to your own internal service. But can you trust third parties? How to verify the resilience of technology provider before allowing him access to your network?

This being the reality, third party interactions are a threat. Everyone has heard of the Solarwinds attack of December last year. The facts:

- more than 18,000 companies were affected
- it came from a cybersecurity provider (Solarwinds service) via a routine update.
- Many companies didn`t know they were breached because they didn`t have logs
- Even US treasury was touched

With this evidence at hands, can we blindly trust our third-party security providers in 2021? And what to do in practice?

Our recommendation: the only way to establish trust is to ask questions. You can get involved with an external auditor - you pay him and trust him for auditing most valuable assets for your company - and, at the same time, you SHOULD also raise your own awareness. Does this seem difficult? At Sirris and Agoria, that is exactly what we work on: try our short free webinars on trust and resilience (to be announced soon in our agenda) or our signature step-by-step hands-on pragmatic masterclasses for digital service builders and outsourcers. We are engaging to provide you with the best learning experience!

You are a digital technology provider?

In 2021, customers are asking questions on cybersecurity and they will ask you even more questions! We have it confirmed that, while working with digital technology providers, whatever technology they provide, the majority of companies receive the following questions from customers:

- Are you secure enough?
- How can I trust you with my data?
- What are the standards you comply with?
- Did you do penetration testing?
- What is your security level?

Being able to answer these questions from the customer is often crucial to close a deal, so trust becomes priority in business continuity for digital service providers. How to do it? There is good news for digital services, and that is, there is a very clear solution: become AppSec. Becoming AppSec simply means applying the principles of secure design from the start, and the principles are very well known as the Application Security Verification Standard. From there on, build your service following the DevSecOps concepts. You can read more about it here and also join our masterclass on cybersecurity for digital service builders!

Authors

Tatiana Galibus