BIZCOMMUNITY

Third-party risks: does your supplier comply?

By Alexey Parfentiev

19 Dec 2019

Make sure your contractors, vendors or partners were "brought up" in the same security-conscious environment your company was.

Alexey Parfentiev is a leading analyst at SearchInform

A company may have the most intelligent approach enveloping each and every facet of your business structure, but as soon as your data is transmitted to a third party you lose control over it. Even if a company is reputable and you've signed all the papers, you're not protected from employee negligence or fraudulent attempt which could take place within the other company's perimeter.

Phineas Fisher, a famous hacker, has recently mentioned mining and livestock companies in South Africa alongside other organisations, mainly banks and oil companies, as the hacktivists' targets. He is willing to inspire others showing them the power of a data breach and reward diligent offenders for data leaks.

The adherent of public interest hacks already compromised surveillance vendors, affected the police, a politic party and a bank claiming the bank's activity was unlawful – he shared the corporate emails with everyone as well as the money which he stole from the bank.

Know who you give your data to

The news came as a reminder of knowing little about the companies we give our data to. We don't know if the third-party business we work with has all the policies and mechanisms in place to prevent an attack or ensure business continuity.

You can’t control a third-party organisation as if it was your own, but you can demand clarity and transparency concerning those areas of activities which involve and might affect your corporate data:

- Your contractor may have a subcontractor. When preparing an agreement make sure you point out the requirement in accordance with which third parties are obliged to inform a company about any external collaborations and sharing confidential data with out-of-contract businesses.

- Be aware of security solutions and privacy policies a contractor introduces and deploys by conducting audit and evaluation.

- Keep track of what agreements you have with third party organisations, which of them access your data and what data they process.

- Keep up-to-date with local and international normative acts and demand that all the contractors do the same. There are different requirements for protection, storage and transfer for various groups of data, and requirements may also vary among data subjects based on their locations as citizenship determines which regulator is to be complied with. All these conditions should be abided by.

Ponemon Institute has conducted research on a third-party data breach issue. In 2016, 49% of companies were affected by a breach due to a contractor, whereas in 2018, there were already 59% of businesses affected indicating the same reason.

The Privileged Access Threat Report 2019, prepared by BeyondTrust, demonstrates that access rights management program and data audit requires enhanced measures.

According to the report, 58% of respondents are sure that they were breached due to third party vendors’ access. A year ago the number of third party vendors which could access organisations’ IT systems reached 75%. 1 in 8 businesses with more than 5,000 staffers employed aren’t even aware of how many vendors access the network remotely in a specific period of time.

Preventative measures needed

As PwC reports, an impressive number of companies have no preventive measures from third-party breaches. Taking into consideration the abovementioned we see that the situation is nearly critical.

Make sure that third parties can’t connect to the assets within your company’s network. Combative network security is crucial as it alleviates the risk of unauthorised access. If a company’s threat mitigation program lacks network segmentation, an organisation is exposed to incidents in case a contractor is breached.

It is important that only the data which is required for work performed by third parties is available to them and nothing which is beyond their responsibilities is exposed. Even if the information isn’t related to the tasks third parties implements but is

available in front of them, it becomes automatically obtainable.

Internal audit should be conducted as an ongoing process in order to monitor deviations from the agreed terms of working, including the amount of data allocated for the third party's use.
It is a company's job to take care of corporate information allotted to a contractor, as they are responsible for task completion, not for information safety, thus, their security measures aren't part of your agreement and might differ considerably from those introduced in your company.

The right to evaluate

You have the right to evaluate a third party's controls and policies relevance which is within the scope of your agreement and conform to the controls and regulations introduced in your company.

The surveillance is obligatory, continuous monitoring procedures of the number of vendors accessing particular systems should be established. Since the access is controlled, the accounts created for the third parties are visible and can be managed.

It is also important to protect both internal and external perimeters - audit of database queries (any databases storing confidential data) is a must, especially considering access from outside, for example, in a corporate CRM.

Healthcare industry can serve an illustration of the consequences of a third-party breach. The largest clients refused to continue working with AMCA (American Medical Collection Agency) due to the breach of personal data which compromised details, including names, dates of birth, provider and balance information, of 20 million U.S. citizens. AMCA, third-party provider of billing services, didn't manage to safeguard the data of major healthcare organisations' clients. The information was exposed from August 2018 until March 2019. The company went bankrupt and announced about it shortly after the incident was discovered.

According to the report made by Gurucul security company, 74% of respondents admit to limiting access granted to third parties - representatives of finance and retail sectors account for 80% of those who narrowed down access rights due to third-party leakage risks.

ABOUT THE AUTHOR

Alexey Parfentiev is a leading analyst at SearchInform - developer of cyber threat mitigation solution.