Date: *March 11, 2019*
Source: *Datensicherheit.de*
https://www.datensicherheit.de/aktuelles/citrix-hack-unternehmen-sicherheit-angriffe-30514

Press Report

After Citrix-hack: no company in the world is immune to attacks – but how can they protect themselves?

A comment by Marc Schieder, CIO DRACOON

[datensicherheit.de, 11.03.2019] It became known last weekend that the US-American software company **Citrix** has become victim of a devastating **cyber-attack**. Citrix is known for being responsible for the processing of **sensitive IT-projects** for the communications agency of the White House, the US-military, the FBI and many American companies. According to a blog entry by the security-provider, the criminals managed to gain access to the internal network and therefore access to business documents. The company itself had not noticed the attack at first; it was the **FBI** which sounded the alarm in this case.

Criminals probably used "password spraying"

According to current information, the IT-security provider was attacked twice within the last few months: once in December and once again last Monday – according to reports by the company **Resecurity**. First information on the perpetrators is already known: The attack is likely to have been executed the Iranian hacker-group Iridium that is also responsible for the most recent wave of cyber-attacks against multiple government agencies, oil and gas companies and other targets. The method used was most likely "**password spraying**". This is not a classic brute-force-attack, but rather a method where typical, common passwords are tried out until the right code is found and access gained. Often very obvious and insecure access information is tried out such as "password". That way, the attackers were able to compromise multiple employee-accounts and infiltrate the network. In total six to ten terabyte of data were probably stolen. As Citrix emphasizes in its blog post on the incident, there are currently no indications that the attack might have consequences for the security of the company products or services. However, according to **NBC News**, due to the particular data sensitivity of Citrix clients, there is a potential risk that hackers could eventually find their way into US-government networks, according to experts.

No company safe from cyber-attacks

The hacker attack against Citrix shows that even companies from the field of IT-security are not safe from unsafe and extremely easy-to-compromise passwords being used internally. This exactly can lead to **large quantities and critical business data** being **compromised**. It poses a risk not only for the company itself but also for its clients. Especially now, companies, regardless of the industry they operate in, need to be more careful not to neglect employee training and high security standards for access information. Furthermore, I recommend introducing a two-factor authentication for the login, this way the access to the accounts is extended by an additional “hurdle”.

Not neglecting risks for IT-security

No company, no matter if global player or medium-sized company, must underestimate the **risks** for **IT-security** – a good protection is no one-off matter, but needs constant monitoring of current dangers and employee training on how to handle them. Apart from internal measures for secure password management and other security strategies, software solutions can also help raise or maintain a high security-level. When implementing a new solution, for example a solution for data exchange – but also other types of software – it is important to ensure that these are already provided with particularly data protection-friendly default settings and that the issues of data security and protection have been incorporated into the development process. The concepts “**Privacy by design**” and “**Privacy by default**” have for some time been among the most frequently discussed issues when it comes to protecting information. In detail they mean nothing other than “data protection by design” as well as “data protection by default”. At least since the anchoring of these principles in the **EU-GDPR** (Article 25), the terms are rightly discussed over and over again and when choosing the right software solutions, these criteria should, or must, absolutely be taken into account.

Raising protection levels

In conclusion, the organizational measures, for example for the secure handling of passwords, as well as special attention paid to data security and protection while choosing software solutions help raise the company’s security level to a maximum. It does not matter whether it is a company in the IT security sector or in another sector. Companies should never underestimate the dangers for their IT-infrastructure.