USER REPORT

Case study: The path to better security leads to the cloud

What can be learned from the REvil ransomware attacks

On November 7, 2020, the managing director of a medium-sized company in Bremen, which operates in the buying and selling of merchandising articles in Germany and France, noticed some discrepancies in the company's internal network. The server data was largely subject to impenetrable encryption. Overnight, a group of hackers well known in IT circles by the name of REvil launched this ransomware attack, which paralysed many of the company's processes for several weeks. The hackers encrypted around 90 per cent of the data and made a high monetary demand of roughly 300,000 Euro for the release of the master key, which authorises the release of any files - a frightening scenario that affects many other small and medium-sized enterprises (SMEs) in Germany and around the world. In recent years, an increasingly alarming rise in cybercrime has developed. While the number of cases in Germany were still at about 82,000 in 2016, the Federal Criminal Police Office has already recorded more than 108,000 attacks for the year 2020.[1]

A cloak-and-dagger operation?

Even though this attack occurred seemingly out of nowhere - which could be traced in retrospect - between one and two o'clock in the morning, it was not a spontaneous action by the cyber criminals. In fact, the CEO suspects that they had already been able to infiltrate the system several weeks earlier. The attack also affected an employee of the company who had been in his home office for a month and simultaneously discovered that his data had been encrypted on his work laptop and could not access important files. This meant that the attack was more widespread than initially assumed and affected practically all of the employees. Only the entry of a six-digit hexadecimal code resolved the issue without losing important data in the process of the attack. For several weeks, the employees had to continue their work with great restrictions, which they managed as good as possible since essential processes could also be carried out manually and could therefore continue to operate as much as possible. In order to keep the economic damage as low as possible, they had to act as quick as possible - easier said than done in view of the acute pressure situation.

[1] Bundeskriminalamt (BKA): Bundeslagebild Cybercrime 2020

Pressekontakt: Borgmeier Public Relations, Niklas Bädjer/Niklas Römer, Lange Str. 112, 27749 Delmenhorst, Tel: 04221-9345-340/-335, Fax: 04221-9345399, baedjer@borgmeier.de/roemer@borgmeier.de

Good guy, bad guy

So what do you do when the worst-case scenario occurs? Many people who are not familiar with IT and are inexperienced in this field have probably already wondered about this on several occasions following the increasing number of reports about cybercrime. In contrast to many movies, in which the blackmailers demand the ransom in a distorted voice and a threatening tone, in reality, such a deal is performed in a much more unimpressive way. In this attack case by the group REvil, only after attempting to access the desired file did a countdown start, which was limited to five days and contained a demand to be paid, which amounted to a total of $300,000 for the affected company. Sums that represent an unmanageable burden for SMEs. After receiving the ransom note, the responsible parties were able to enter into chat communication with the criminals and negotiate the ransom. In the process, it crystallized that they were dealing with multiple perpetrators on the other side during the tough negotiations that lasted several days. On one side an unyielding, tough negotiator and on the other a communicative, friendly person with whom a compromise could be reached. For a much smaller sum, they finally reached an agreement in the negotiations. Since no alternative solution emerged to recover the valuable data collection of over 20 years of successful entrepreneurship, the management settled the amount with the non-traceable cryptocurrency Monero.

Control beats trust

Following the zero-trust approach, the management then investigated all structures and processes in order to identify security gaps in the network as precisely as possible. For assistance, the managing director hired a local IT security company from Bremen to assess the situation with their many years of experience and accumulated expertise in this area. The management was not able to follow the advice of the security experts to completely replace the entire hardware, as the financial framework conditions did not make it possible. The responsible insurance company also did not provide a favourable response in terms of financial support, which led to the company's decision to build a new IT infrastructure. Based on trust, the company eventually contracted the data centre service provider firstcolo, which operates its own data centres and provides colocation and managed services for a number of different clients. The two parties first made contact in mid-December 2020. In the course of further cooperation, the company moved its data sets to firstcolo's external data centre and is now managing them from the cloud.

Pressekontakt: Borgmeier Public Relations, Niklas Bädjer/Niklas Römer, Lange Str. 112, 27749 Delmenhorst, Tel: 04221-9345-340/-335, Fax: 04221-9345399, baedjer@borgmeier.de/roemer@borgmeier.de

USER REPORT

Ascent into the Cloud

Especially for medium-sized and small companies, the outsourcing of servers and data provides many advantages. In terms of security, a migration from on-site internal data storage to external data centres makes perfect sense, as service providers such as firstcolo can monitor the servers, which are often rented, 24/7 and therefore ensure an all-round monitoring of the systems. Administrative tasks and maintenance work are no longer part of the in-house area of responsibility, which in return results in more effective processes and financial savings. Hardware, which has to be replaced every three to five years in the case of intensively used servers, no longer represents a cost factor for the company renting it. Especially as a result of the Corona pandemic, flexible working models are playing an increasingly important role. Whether in an office located at different sites or in a home office, the cloud application can be used flexibly from any location. In addition, employees can access information or make changes to the system securely.

Ignorance does not protect from punishment

In order to avoid a cyber attack in the future, the company not only established the new IT structure, but also took further measures to sensitise the employees - the core users of the system. Typically, cyber criminals gain access to an existing system through a single user, presumably as in this case. This is exactly where the responsible authorities started immediately after the attack, in order to minimise one of the biggest entry points in an otherwise secure network. For this purpose, they designed a security training programme for their employees, which can be completed independently through a security platform they developed themselves. It contains comprehensive training material and a final test, after which each user receives a certificate. A major issue remains the often underestimated phishing e-mails, which still tempt many users to fall for traps set by criminals and thus expose ongoing business operations to great risk. The security training paired with data storage in the cloud by firstcolo results in an IT infrastructure that offers cyber criminals almost no chance of access in the future. Further attacks can therefore be proactively prevented resulting in a risk-free operation of the company's critical IT.

Further information about diva-e Datacenters GmbH can be found under first-colo.net.

Pressekontakt: Borgmeier Public Relations, Niklas Bädjer/Niklas Römer, Lange Str. 112, 27749 Delmenhorst, Tel: 04221-9345-340/-335, Fax: 04221-9345399, baedjer@borgmeier.de/roemer@borgmeier.de

USER REPORT

firstcolo

As an operator of data centres in Germany, firstcolo, based in Frankfurt am Main, provides its customers with the highest level of service quality. In addition to classic colocation and the rental of server systems, firstcolo's range of services also includes storage-on-demand solutions, backup solutions and cloud services. firstcolo is part of the diva-e Group, which, as the leading transactional experience partner in Germany, has over 20 years of industry expertise in the digital world. Around 800 diva-e Group employees in 13 offices in 8 different locations take care of the needs of the wide-ranging customer base, which includes a large pool of industries from technology, retail and healthcare. In addition to large and well-known companies such as FC Bayern Munich, Siemens, Mister Spex, Audi or Sky, many other renowned customers are among them.

Pressekontakt: Borgmeier Public Relations, Niklas Bädjer/Niklas Römer, Lange Str. 112, 27749 Delmenhorst, Tel: 04221-9345-340/-335, Fax: 04221-9345399, baedjer@borgmeier.de/roemer@borgmeier.de