DRACOON

Date: *July 19, 2019*
Source: *it-daily.net*
https://www.it-daily.net/it-sicherheit/cyber-defence/21901-erneuter-ransomware-fall-in-deutschen-krankenhaeusern

Press Report

Once again, ransomware-attack in German hospitals – hazardous situation remains

After a renewed ransomware case in German hospitals, the hazardous situation remains. A statement by Arved Graf von Stackelberg, Managing Director Dracoon.

As several media reported last Wednesday, the sponsorship South-West of the German Red Cross (Trägerschaft Süd-West des Deutschen Roten Kreuzes) has fallen victim to an attack with an encryption trojan. In total, this concerns 13 clinics, a large part of which are located between Mannheim and Bonn, and two others close to the borders with France and Luxembourg. The attack was discovered on Sunday morning; the malware had encrypted the server as well as the databases. As a reaction, the servers were taken offline on Sunday afternoon to check them for infestation and to prevent further spreading of the malware. The encryption process could thus be stopped in the afternoon, according to the hospital sponsorship. The State Criminal Investigation Office was notified, and a complaint was filed, according to the spokesperson for the sponsorship. Even though there was no specific ransom demand, an email including a text file was received – however, it was transferred to the State Criminal Investigation Office unopened. It can be assumed that this was the claim. As a consequence of the attack, the affected clinics were at times completely cut off from the Internet and could not be reached by email, telephone or fax.

Large scale spam campaigns

The incident shows that Ransomware is still a major threat to German organizations about two years after WannaCry – not only for CRITIS companies. A recently published study by the auditing and consulting network KPMG "E-Crime in the German economy" confirms this. For the survey, 1,000 companies in Germany, including those from the healthcare, trade and industry sectors, were asked about their experiences with cybercrime. Here it becomes clear that every third company (31 percent) in the last two years has already been the victim of an attack with an encryption trojan. This is twice as many as in the previous KPMG survey. A further 28 percent reported attempts to introduce ransomware into the systems. According to the publication, large companies in particular have seen a significant increase in attacks. In view of these figures, it is not surprising that the BSI (Federal Office for Information Security) again warned against targeted ransomware attacks on companies in a press release this April. According to the agency, a popular and currently widespread attack technique is the sending

of large-scale spam campaigns, such as Emotet, to first gain access to individual corporate networks and then manually explore the network and systems of those affected. Here, the criminals try to manipulate or delete backups and then selectively distribute ransomware on the computer systems in a coordinated manner for particularly lucrative targets. The consequences are sometimes massive operational interruptions, and in addition, the perpetrators can make significantly higher ransom demands than in unspecific ransomware campaigns.

Integrated ransomware protection

In times of increasing threats in the field of ransomware, companies urgently need to be prepared. In case of an infestation the BSI advises against meeting the demands of the blackmailers. Furthermore, companies should inform their business partners and clients as soon as possible and point out possible attempts to attack by email using fake senders from their company. However, companies are best advised to make sure that an attack is futile, and that business data is not in danger. This is where companies should take a close look at their in-house software, such as the cloud storage solution they use. Ideally this is equipped with an integrated storage ransomware protection (such as a recycle bin with versioning) that ensures that the data is not affected during an encryption attack. Should ransomware encrypt local drives or network drives despite all precautions, companies still do not lose any files thanks to the versioning of the recycle bin. During a ransomware attack all data is overwritten with the encrypted data – the unencrypted version of the data is automatically stored in the recycle bin and can be restored completely and unharmed. Thus, the loss of data can be prevented from the start. The BSI-KRITIS regulation, which came into force end of June this year and is binding for numerous German clinics, also states that hospitals affected must comply with the latest technology with regard to their IT infrastructure. It is important to ensure that an attack of any kind on a single system does not immediately affect the entire network. The protection mechanisms of the computer networks must prevent that. Here, too, a feature is applied that curbs a ransomware attack and with which the damaged data can be restored promptly. Overall, even two years after the historic WannaCry wave, companies need to be prepared that attackers act even more professional and insidious to do maximum damage and therefore need to adjust their security levels.