DRACOON

Date: *February 21, 2019*
Source: *it-daily.net*
https://www.it-daily.net/it-sicherheit/enterprise-security/20678-im-visier-von-hackern-nehmen-kritis-betreiber-die-gefahr-ernst-genug

Press Report

Targeted by hackers – Are critical infrastructure providers taking the danger seriously enough?

According to Research by the WELT AM SONNTAG, security authorities registered a considerable increase in attacks against the IT infrastructure of organisations, compared to last year. A comment by Marc Schieder, CIO DRACOON GmbH:

The attacks, presumably often led by foreign secret services, have changed. Recently, extorting money has become less frequent – the aim has rather been to disrupt business operations as effectively as possible. For example, water and power supplies are being manipulated. According to the German Federal Office for Information Security (BSI) the attacks have reached a new level of quality. Even if not every malfunction can be blamed on a hack, as the BSI emphasises, the number of incidents has risen considerably – from 145 in the reporting period of June 2017 to end of May 2018 to 157 in the second half of the year 2018. 19 of these attacks affected the energy sector.

This rise is alarming, considering the high sensitivity of the affected sectors – since a possible break-down would endanger security, health and social welfare of the population. But how do providers themselves assess the situation? In the middle of last year, the project VeSiKi (Vernetzte IT-Sicherheit Kritischer Infrastrukturen) an accompanying project of the research focus ITS/KRITIS by the Federal Ministry of Education and Research, published the report “Monitor 2.0 – IT-Sicherheit Kritscher Infrastrukturen” (Monitor 2.0 – IT security of critical infrastructures).

CISOs, CIOs, other management members and IT security officials from critical infrastructure sectors such as water supply, information and communication technology, energy and health were interviewed – but also SMEs and companies with more than 250 employees. The publication clearly shows that critical infrastructure providers often assess their security optimistically and feel secure.

Nevertheless, it also shows that all in all the participants do take the danger seriously. When asked for an assessment of the threat situation in the area of cyber security, differentiated according to the economic area Germany, the own industry, and the own organization, the threat was constantly described as “high” or “very high”.

However, the threat situation was judged to be smaller for the own organisation as opposed to the other ones for the sector in question or for Germany as a whole. The danger for the

whole of Germany was judged to be very high by 35% and high by 65% – when looking at individual sectors it was 15% (very high), 70% (high) and further 15% (low).

The most positive evaluation was the one of the own organisation: 10% do see a very high danger, a little over 70% see a high risk potential, but nearly 20% believe there is only little danger.

To be prepared against future dangers for the IT-security, providers in the field of critical infrastructure need to constantly keep their protection levels high and must never underestimate the dangers. Furthermore, software developers acting as providers in the field of critical infrastructure need to take their responsibility seriously and incorporate the high data sensitivity in their products.

This includes having the products independently tested. Here for example the ISO 27001 or the European Privacy Seal (EuroPriSe) are to be mentioned. Moreover, features such as client-side encryption and a well-thought-out user rights system, enabling certain persons to access data or to deny them access, ensure maximum data security from the start.

Overall, those responsible in the field of critical infrastructure seem to have high safety awareness. However the safety measures need to be constantly adapted and increased in light of reoccurring security incidents within the last few months. In addition to the creation of a culture of security within the company through education and training, this also includes the implementation of solutions whose manufacturers have already incorporated the high threat potential into their products during development.

www.dracoon.com