DRACOON

***Date:*** *January 31, 2019*
***Source:*** *SECTANK*
*hhttps://sectank.net/2019/01/31/weltwirtschaftsforum-warnt-erneut-vor-wachsenden-gefahren-fuer-die-cybersicherheit-unternehmen-koennen-kritische-daten-nicht-mehr-selbst-schuetzen/*

Press Report

# Once again, the world economic forum warns of growing dangers for cyber security: companies can no longer protect critical data themselves

A Statement by Arved Graf von Stackelberg, CSO at DRACOON

Last Friday the 49th annual meeting of the Word Economic Forum (WEF) ended in Davos. This year the meeting's motto was "Globalization 4.0: Shaping a Global Architecture in the Age of the Fourth Industrial Revolution". The risk report published during the meeting, which was presented in London last week, highlights the biggest threats the world faces today. Next to climate change, geopolitical crisis and worldwide economical tensions, data fraud and theft as well as cyberattacks are some of the worldwide biggest risks.

The topic of IT security has been perceived and presented as a problem in Davos for several years in a row, but there has been little change in the risk potential. On the contrary, companies are faced with a constantly growing attack surface, for which there are three main reasons. For one, the attack vectors have been increasing just as quickly as the constantly advancing network in course of the IoT. Furthermore, the expertise within the development and programming departments of software manufacturers has often not kept pace with rapid technical progress. As a result, more and more unsafe code is created – a further risk. The continuing shortage of IT security specialists is also a further factor. Companies, both large corporations and SMEs, can no longer control this situation with their own resources.

To master the situation, companies need to acknowledge the fact that they cannot solve this problem alone. The next step should be to think about how this understanding can at least ensure the secure operation of mission-critical data and communications in environments that have been created specifically for this purpose and provide a higher level of security than our economy can currently provide.

Ideally, the critical data should be stored in a highly secure cloud or hybrid environment. Solutions using a consequent end-to-end encryption offer a maximum of security. Ideally, it is provided as an open source so the administrator can convince himself of the completeness of the solution. Furthermore, a modern authorization concept is important to ensure that only intended people have access to the corresponding data. To keep the information controllable within the national boarders, it is important that the server is hosted within Europe. Unlike foreign providers, a solution developed in Germany guarantees strict compliance with the German jurisdiction for data security and data protection. To be on the safe side, it is therefore advisable for enterprises to use software "Made in Germany" that

has the corresponding data protection certifications. Next to the international Norm ISO 27001, further certifications in this context are for example the European Privacy Seal EuroPriSe and the data protection seal for “Hervorragenden Datenschutz nach deutschem Recht” (excellent data protection in accordance with the German law) from the ULD (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein).

In order to live up to the constantly growing risk potential, companies should be sure to use secure cloud solutions for their highly sensitive information and not compromise their security choices. After all, real security can only be guaranteed if it is the central focus of an organization – and currently the German economy is not able to ensure that for its own data due to the reasons stated above.

For more information about DRACOON visit: https://www.dracoon.com/