Statement on the Security Gaps “Meltdown” and “Spectre”

Retarus assesses level of threat to its customers to be low

Munich, January 12, 2018 – At the moment an increasing number of discussions are appearing in the media about the hardware-based security vulnerabilities “Meltdown” and “Spectre”. These flaws in the architecture of practically all modern processors allow access to information in other processes running on the same hardware, which should actually be secure. In the corporate environment this can lead to severe security breaches, particularly in multi-client or multi-purpose systems. A precondition for this, however, is that the attacker is already in a position to execute code on the system.

Retarus provides its services according to the SaaS model (Software-as-a-Service). There are no external parties with direct access to the system, which is shielded from outside intrusion. The hardening of the system to prevent the embedding of code by a third party in any way or form, is an essential component of the entire system architecture and has been tested by independent, external security experts. Granularization furthermore secures Retarus’ systems against attacks such as “Meltdown” and “Spectre”. Each system only fulfills a single function as far as possible. Thanks to this multi-layered security architecture, Retarus rates the current threat level as being low.

In order to ensure that this far-reaching security separation continues over the long term, Retarus is taking additional precautionary measures. For all system components in use, any alerts and notifications received from the respective manufacturers are followed precisely, while both recommended actions and patches are immediately passed on the service operations. In accordance with the Standard Patch Management, security patches are assessed in terms of importance and their impact on the service, tested and then rolled out. In this way, risks caused by known vectors of attack are eliminated at an early stage. If this is expected to lead to any downtime for the services, Retarus’ customers will as usual be informed with sufficient lead time. What’s more, Retarus’ Intrusion Detection and Prevention System (IDS/IPS) regularly undergoes training using known patterns of attack. This facilitates the early detection and potential blocking of any attacks which may seek to target the new processor vulnerabilities.

About Retarus

Since 1992, Retarus has been supporting companies in achieving highly efficient communication. The global information logistics provider always plays an important role where large amounts of data need to be transmitted securely and reliably - irrespective of which communication channels, interfaces, applications and devices are required. The services are soundly based on a Global Delivery Network which includes the company's own data centres in Europe, the USA and the APAC region, as well as redundant carrier infrastructure. Half of all EURO STOXX 50 companies and 17 percent of Dow Jones corporations depend on Retarus' services. Longstanding customers include Adidas, Bayer, Continental, DHL, DZ Bank, Honda, Linde, Osram, Puma, Sixt, Sony and Thomas Cook. For more details: www.retarus.com