# Kaspersky Lab moving core infrastructure from Russia to Switzerland; opening first Transparency Center

As part of its Global Transparency Initiative, Kaspersky Lab is adapting its infrastructure to move a number of core processes from Russia to Switzerland. This includes customer data storage and processing for most regions, as well as software assembly, including threat detection updates. To ensure full transparency and integrity, Kaspersky Lab is arranging for this activity to be supervised by an independent third party, also based in Switzerland.

Global transparency and collaboration for an ultra-connected world

The Global Transparency Initiative, announced in October 2017, reflects Kaspersky Lab's ongoing commitment to assuring the integrity and trustworthiness of its products. The new measures are the next steps in the development of the initiative, but they also reflect the company's commitment to working with others to address the growing challenges of industry fragmentation and a breakdown of trust. Trust is essential in cybersecurity, and Kaspersky Lab understands that trust is not a given; it must be repeatedly earned through transparency and accountability.

The new measures comprise the move of data storage and processing for a number of regions, the relocation of software assembly and the opening of the first Transparency Center.

Relocation of customer data storage and processing

By the end of 2019, Kaspersky Lab will have established a data center in Zurich and in this facility will store and process all information for users in Europe, North America, Singapore, Australia, Japan and South Korea, with more countries to follow. This information is shared voluntarily by users with the Kaspersky Security Network (KSN) an advanced, cloud-based system that automatically processes cyberthreat-related data.

Relocation of software assembly

Kaspersky Lab will relocate to Zurich its 'software build conveyer' — a set of programming tools used to assemble ready to use software out of source code. Before the end of 2018, Kaspersky Lab products and threat detection rule databases (AV databases) will start to be assembled and signed with a digital signature in Switzerland, before being distributed to the endpoints of customers worldwide. The relocation will ensure that all newly assembled software can be verified by an independent organization, and show that software builds and updates received by customers match the source code provided for audit.

Establishment of the first Transparency Center

The source code of Kaspersky Lab products and software updates will be available for review by responsible stakeholders in a dedicated Transparency Center that will also be hosted in Switzerland and is expected to open this year. This approach will further show that generation after generation of Kaspersky Lab products were built and used for one purpose only: protecting the company's customers from cyberthreats.

Independent supervision and review

Kaspersky Lab is arranging for the data storage and processing, software assembly, and source code to be independently supervised by a third party qualified to conduct technical software reviews. Since transparency and trust are becoming universal requirements across the cybersecurity industry, Kaspersky Lab supports the creation of a new, non-profit organization to take on this responsibility, not just for the company, but for other partners and members who wish to join.

Kaspersky Lab's commitment

As a leading global cybersecurity solutions provider, Kaspersky Lab has always been committed to the most trustworthy industry practices, including strong protection for transmitted data, strict internal policies for data access, ongoing security testing of its infrastructure, and more. With this new set of measures, Kaspersky Lab aims to significantly improve the resilience of its IT infrastructure to any trust risk – even theoretical ones – and to increase its transparency to current and future clients as well as to the general public.

Commenting on the process move and transparency center opening, Eugene Kaspersky, CEO of Kaspersky Lab, said: “In a rapidly changing industry such as ours we have to adapt to the evolving needs of our clients, stakeholders and partners. Transparency is one such need, and that is why we’ve decided to redesign our infrastructure and move our data processing facilities to Switzerland. We believe such action will become a global trend for cybersecurity, and that a policy of trust will catch on across the industry as a key basic requirement.”

Learn more about Kaspersky Lab transparency principles and the Global Transparency Initiative here: www.kaspersky.com/about/transparency

Notes to editors

On June 5, Kaspersky Lab will be hosting a live online summit, bringing together senior representatives from the cybersecurity industry to discuss how to maintain trust and collaboration across the industry and address the growing challenge of Balkanization. Further details and registration can be found https://kas.pr/xzr9