Collateral Damage – on Cybersecurity

In the last three weeks, the war in Ukraine has shattered the world we knew. Families, relations, partnerships, and ties were affected dramatically in Ukraine, Russia, Europe and the entire world. The avalanche of these tragic events catches us all.

It has also caught my company, the world's largest private cybersecurity business that proudly bears my name. This week the German Federal Office of Information Security (BSI) issued a warning about Kaspersky products, citing potential risks for IT security of those using Kaspersky products and solutions. Without going into details I can say that these claims are speculations not supported by any objective evidence nor offering technical details. The reason is simple. No evidence of Kaspersky use or abuse for malicious purpose has ever been discovered and proven in the company's twenty-five years' history notwithstanding countless attempts to do so.

Without such evidence, I can only conclude that BSI's decision is made on political grounds alone. It is sadly ironic that the organization advocating for objectivity, transparency, and technical competence – the very same values Kaspersky supported for years together with BSI and other European regulators and industry bodies – decided or was forced to drop its principles literally overnight. Kaspersky, the long-time partner and contributor of BSI and German cybersecurity industry, was given mere hours to address these bogus and unfounded allegations. This is not an invitation for dialogue – it is an insult.

Despite continuous calls from Kaspersky to conduct a deep audit of our source code, updates, architecture and processes at Kaspersky Transparency Centers in Europe, BSI has never done so. This decision also conveniently omits the fact that Kaspersky has for years pioneered greater transparency with a multi-million euro effort of relocating the threat data of our European customers to Switzerland as a part of our Global Transparency Initiative. That is why I consider the BSI decision as an unwarranted and unjust attack on my company and specifically on Kaspersky employees in Germany and Europe. More importantly this is also an attack on the large consumer base in Germany trusting Kaspersky, which two weeks ago was awarded as the best security offering (by AV-Test). It is also an attack on the jobs of thousands of German IT security professionals, on law enforcement officers we have trained to combat cutting-edge cybercrime, on German computer science students we have helped obtain job-ready skills, on our partners in research projects in the most critical areas of cybersecurity, and on tens of thousands of German and European businesses of all sizes which we have been protecting from the whole spectrum of cyberattacks.

The reputational and business damage of the BSI decision is already quite significant. The only question I have – to what end? Not having Kaspersky in Germany will not make Germany or Europe safer. Quite the contrary. The BSI decision means that German users are strongly advised to immediately uninstall the only antivirus that according to AV-Test, an independent German IT-Security Institute, guarantees 100% protection from ransomware. This means that the leading German industrial equipment manufacturers will no longer receive information about critical vulnerabilities in their software and hardware from Kaspersky ICS-CERT – an organization hailed for its responsible disclosure work by these very same manufacturers. This means that German automotive giants will remain oblivious to the bugs that may allow an attacker to overtake the entire on-board computer system and change its logic. This means a huge blind spot on the attack surface for European incident responders and SOC operators, who will no longer be able to receive threat data from across the globe – and from Russia in particular.

My message to BSI, which now seems to be avoiding contacts with our German team, is simple: we consider this decision to be unfair and outright wrong. Nonetheless, we remain open to addressing any concerns you may have in an objective, technical, and honest manner. We are thankful to the European regulators and industry experts who have taken a more balanced approach by calling for additional technical analysis and scrutiny of security solutions and the IT supply chain, and I am fully committed to providing all the information and cooperation that is required from Kaspersky throughout this process.

And to our German and European customers I want to say that we are immensely grateful for your choice of Kaspersky, and that we will continue to do what we do best – protecting you from all cyberthreats no matter where they are coming from, while being fully transparent with regard to our technology and operations.

The war in Ukraine can only end through diplomacy, and we are all hoping for a cessation of hostilities and continuing dialogue. This war is a tragedy that has already brought suffering to innocent people and repercussions across our hyper-connected world. The global cybersecurity industry that has been built on the basis of trust and cooperation to protect the digital links connecting us with each other may well be its collateral damage – and thus leave everyone even less safe.