TUM THINK TANK

Digital Sovereignty Talks

Food4Thought

Summer 2024

Munich School of Politics and Public Policy (HfP) · TUM Think Tank

v1.4

What We Learned from the CrowdStrike Incident: A Question of Philosophy, Not Sovereignty?

By Udo Riedel and Philipp Mueller

The recent CrowdStrike incident has often been framed as an issue of digital sovereignty. While this is not entirely wrong, we believe it represents a deeper philosophical question about how we approach cybersecurity in our increasingly interconnected world.

The recent CrowdStrike incident has often been framed as an issue of digital sovereignty. While this is not entirely wrong, we believe it represents a deeper philosophical question about how we approach cybersecurity in our increasingly interconnected world.

The incident itself was digital in nature, had territorial implications, and caused systemic disruptions (such as airport closures), to use Christian Laux's definition of digital sovereignty. This understandably led to sovereignty concerns. However, given the lack of a clear strategic actor or adversary behind the incident, it seems more accurate to view it as a manifestation of the inherent risks of a particular philosophy of how to defend an organization in cyberspace: the country of origin of CrowdStrike or any similar cybersecurity firm was less relevant in this case than the underlying philosophy guiding their approach to securing customers.

Alternatively, we can frame the incident in terms of what philosophies of cybersecurity are at work, similar to the different approaches military strategists use to secure their countries.

CrowdStrike's philosophy, which could be described as recognition-based or "interventionist defense," involves deeply integrating into all layers of an organization's tech stack. This enables them to identify patterns and respond to threats with remarkable speed. Customers place immense trust in this system, and it generally proves effective.

However, this "interventionist" philosophy presents three significant challenges:

- Total Trust Requirement: Customers must entrust CrowdStrike with complete access to their systems. This means opening up all their technological assets to an external entity and constantly uploading samples to the threat intelligence in the cloud.
- Risk of System Disruption: Granting CrowdStrike deep, automatic access on all layers of an organization's tech stack introduces the risk of unintentional disruptions or failures within the system.

- Frequent Updates and Their Risks: The constant patching necessary to counteract new threats increases the need for frequent and automatic updates. Given the inevitability of software bugs, more updates correlate with a higher probability of something breaking.

So, what’s the alternative? Consider a different philosophy: a “protective” approach, accepting that in a complex world, we can never recognize all potential dangers and, therefore, need to defend against the unknown. This can be done by ensuring the integrity of the existing system by allowing a set of programs and program behaviors and stopping everything else. In this way of framing the world, only pre-approved software is allowed to execute, based on a “golden image” of the organization’s tech stack. Here’s how it works:

- Access Limitation: This approach does not require access to all layers of the tech stack, significantly reducing potential vulnerabilities.
- Simplicity and Manageability: It’s easier to manage since it doesn’t necessitate deep system integration and requires drastically less updates.
- Controlled Changes: While the system needs to evolve over time, changes can be managed through a carefully vetted process, whether by designated authorities or by documenting user actions.

This protective defense strategy offers several advantages. It provides robust security without the need for deep access, minimizes the risk of system disruptions, and is easier to maintain due to the reduced need for updates.

In conclusion, the CrowdStrike incident should prompt us to reconsider not just our digital sovereignty but the fundamental philosophies driving our cybersecurity strategies. Do we prefer the active, integrated approach with its rapid responsiveness but higher risks? Or do we adopt a more passive, controlled model that emphasizes stability and simplicity? Both have their merits, and the right choice will depend on the specific needs and risk tolerance of each organization.

Ultimately, this isn’t just about digital sovereignty—it’s about choosing the right digital philosophy for our future.