UNiSCON
Sealed Cloud Technologies
A member of TÜV

A risk to the supply chain: Secure systems with Sealed Platform?

July 25, 2019 – Munich: A £183m fine was not what the directors of British Airways (BA) had been expecting. Owing to the GDPR, data breaches can end up being quite expensive—something the UK airline is now discovering for itself[1]. And this figure doesn't even quantify the loss of image! You may recall that in 2018 details of about 500,000 customers had been harvested by hackers. Now, almost a year later, BA is being forced to pay up—and the data theft is costing it a pretty penny!

Companies that use the services of Indian tech service provider Wipro and thus violate their data protection obligations are also facing severe penalties[2]. Since 2017, the IT supplier has increasingly been the target of cybercriminals, who home in on Wipro's customers, among them Internet providers, insurance companies, and energy utilities.

What is the common denominator in these two cases? Weaknesses in the supply chain—a risk that many suppliers and companies underestimate. But how to avoid them?

Risks inherent in supply chain management

The primary goal of supply chain management is optimizing all processes along the entire supply and value chain. Ideally, suitable interfaces are available to the partners for this purpose; in addition, there is a high level of trust between the companies involved, allowing suppliers and customers to learn about problems in their own supply chains, for instance.

Even so, disruptions occur time and again. Apart from those that may arise in the value chain itself, such as short-term delivery bottlenecks or production stoppages[3], these are mostly data protection incidents.

This is because suppliers must be able to access a company's data and frequently also share additional information with employees, which broadens the scope for hackers and cyber criminals to attack. Another risk is that internal attackers—staff or administrators, for example—may gain unauthorized access to confidential information and steal, damage or manipulate it.

How does secure supply chain management work?

To minimize risks and avoid costly data breaches from the outset, companies should secure their supply chain—in the same way as all data processing systems must be adequately protected. This goes not just for the software, but especially for the underlying infrastructure.

Whether companies and suppliers use third-party cloud offerings or their own server infrastructures is irrelevant—the vulnerabilities are generally the same. Operators often rely on a combination of "technical and organizational measures"[4] to protect data from attack and loss. However, there is always a risk that the organizational measures could be circumvented and that employees of the operator or administrators could gain unauthorized access to sensitive data.

---

[1] https://www.bbc.com/news/business-48905907
[2] https://www.forbes.com/sites/kateoflahertyuk/2019/04/16/breaking-down-the-wipro-breach-and-what-it-means-for-supply-chain-security/#442914205259
[3] https://www.riskmethods.net/media/Content/Whitepapers/bme-lieferkette-so-mindern-sie-risiken.pdf (German only)
[4] https://gdpr-info.eu/art-32-gdpr/

Sealed Platform: security through sealing?

The good news is that there *is* a safer approach! Sealed infrastructures like Uniscon's Sealed Platform provide greater protection than conventional clouds and server systems. Instead of combining technical and organizational measures, the Munich-based TÜV SÜD subsidiary relies on a set of purely technical protective measures. They are almost impossible to circumvent even with considerable effort—not even by the server operator or administrators.

This is achieved, for one thing, with cages protected by sensors, a hardened operating system, and interfaces with special filters. An elaborate sealing process with independent checkpoints ultimately safeguards the integrity of the servers and, in turn, the integrity of the data stored and processed on these.

Uniscon's ultra-secure cloud platform ensures that secure software is not compromised by gaps in the infrastructure. Thus, supply chain management applications can be secured to such an extent that unauthorized data access is virtually impossible, allowing companies to avoid big penalties like the one imposed on British Airways.

Further information on the Sealed Platform and printable images are available on request from presse@uniscon.de.

Uniscon—a company of the TÜV SÜD Group

Uniscon GmbH is a company of the TÜV SÜD Group. As part of TÜV SÜD's digitalization strategy, Uniscon provides high-security cloud applications and solutions for secure, legally compliant data traffic. TÜV SÜD is one of the world's leading technical service providers with over 150 years of industry-specific experience and more than 24,000 employees at around 1,000 locations in 54 countries. Within this strong network, Uniscon is able to reliably implement large-scale international projects in the IoT and Industry 4.0 sectors with the Sealed Cloud and its products.

Further information on partners and products: www.uniscon.com

Press contact

Uniscon GmbH, Claudia Seidl
Ridlerstr. 57
80339 Munich (Germany)
email: presse@uniscon.de
Internet: www.uniscon.com
Phone: +49 (0)89 / 41 615 988 104

Kafka Communication GmbH & Co KG, Julia Fehrle
Auf der Eierwiese 1
82031 Grünwald (Germany)
Phone: +49 (0)89 74747058-0
Fax: +49 (0)89 74747058-20