In 2023, Colombia has witnessed a significant surge in ransomware attacks. We have observed how this type of threat has targeted entities ranging from private health sector companies to the General Prosecutor's Office, the Medellín metro, and other public entities in the same city.

Recently, an attack was directed at the supply chain, specifically targeting cloud service providers. IFX Networks, a pivotal provider for governmental entities and private companies in Colombia, was the victim of this assault. It also spread to neighboring countries such as Chile, Argentina, and Panama, marking it as one of the largest incidents in the region.

The Colombian government has been especially hard hit. For over a week, essential systems for the functioning of the judiciary branch and for the provision of health services in the country have been experiencing issues. The restoration process appears to be less than effective.

IFX Networks has been notably tight-lipped about the attack, offering scant information to the media. Their cooperation with the government seems far from what was expected. This incident not only raises the risk of Colombian citizens' information being leaked, but it also highlights structural problems in how both governmental entities and private companies face cybersecurity challenges.

Questionable Trust in Enterprise Software

VMWARE stands out as a significant example. Earlier in the year, security experts sounded alarms about vulnerabilities within the platform, including its ESXI software and other applications. Situations experienced by companies like IFX and MGM highlight negligence in handling security updates, representing a risk for its users.

Many organizations, including the government, believe that using such software will provide better support and security. However, what happens is that they become integrated into a service outsourcing chain, which adversely impacts their system's security.

Outsourcing Technology: Solution or Problem?

The situation with IFX underscores the risks of over-relying on third parties. Facing problems with a company like IFX can lead to catastrophic consequences for the government, potentially jeopardizing national security. It's crucial for state entities to maintain control over their technological infrastructure.

The Issue with Certifications

Many companies, like IFX, invest in security certifications. However, recent events suggest that these certifications may be mere window dressing. It's essential to ensure that, beyond having the certifications, companies apply the best recommended practices.

The Potential of Open Source Software

A technical solution might lie in open-source software. Although it presents challenges in terms of usability, its benefits, such as adaptability and transparency, are invaluable. Moreover, they allow for faster cycles of security patch implementation and improvements.

Despite the benefits of open-source software, the ransomware issue won't be solved solely with technology. It's also vital that organizations adequately train their staff on security matters and follow best practices. Choosing more flexible and customizable technologies can significantly increase the security level.

Refs:

- https://osintcorp.net/hackers-behind-mgm-cyberattack-thrash-the-casinos-incident-response/
- https://osintcorp.net/hackers-behind-mgm-cyberattack-thrash-the-casinos-incident-response/
- https://csirt.gob.cl/noticias/10cnd23-00108-02/
- https://muchohacker.lol/2023/09/pequena-y-mediana-empresa-victimas-invisibles-de-incidente-digital-de-ifx/
- https://muchohacker.lol/2023/09/lista-de-sitios-web-con-el-dominio-go-co-que-estarian-afectados-por-ataque-ransomware-a-ifx-network/
- https://muchohacker.lol/2023/09/medidas-de-seguridad-basicas-para-no-expertos-que-se-deben-tener-en-cuenta-debido-al-ataque-a-ifx-networks/