Cyber Attacks in the Automotive Industry – Sales Approach

December, 2019

find out more at **sikur.com**

Abstract

The purpose of this document is to support the Sikur Sales team when approaching the Automotive market. As Sikur is getting more aware of specific threats in the most diverse markets, and doing its homework to serve them well, there are different ways to mitigate risks related to the communication for this Industry.

No organization can perform tasks without communicating, and in the digital era, mobile devices are the way to go. Desktop and laptop should not be left behind, as it still prevails, but the mobile wave is massive and should grow in the years to come.

The Industry Fears

Let's face it: the truth is that companies and governments do communicate using the wrong channels. That hidden nightmare come true when sensitive information comes out in the news and C-Level's start packing their stuff to leave the office. Malware, ransomware, phishing, and a variety of threats can be hard to fight, but there are very good tools to – at least – force the less-persistent hackers moving to the easiest target.

A couple of years ago, the ransomware was a huge fear, big companies paying to get their data back. But sadly, it still happens, and people still pay to get their data — a huge mess. Malware is always around, silently obtaining data, or using the device's processor and memory resources for crypto mining or even to attack others, making a zombie device. From the organizational perspective, where a considerable number of devices (sometimes unmanaged) vulnerable and freely exchanging sensitive information, it is a recipe for disaster.

The automotive should be afraid. As the FBI recently warned (1), the automotive industry is also facing other types of threats, including but not limited to data destruction following ransomware attacks and persistent unauthorized access to their enterprise networks.

Sales Approach

Although Sikur is getting prepared to server Industries, like the Automotive, with SikurOS, SDK, App Store, and IoT, the way to go now is the SIKUR Messenger.

SIKUR Messenger, with its Cloud business models, provides a high value for enterprise communication, and for the Automotive industry, it is even truer due to the amount of sensitive information that goes back and forth around the globe.

The recent merger between FCA and PSA group (2), while keeping the companies group independence in regard to brand, it will create a global powerhouse competing with the likes of Volkswagen, Nissan-Renault and Toyota, producing annual vehicle sales of 8.7 million, revenues of $189.54 billion (170 billion euro), $12.26 billion (11 billion euro) in recurring operating profit and an operating profit margin of more than 6.6% based on 2018 results, according to the companies.

How does the above group of companies communicate and send their sensitive information? Are they using e-mail systems, WhatsApp, Telegram? For sure, there is a weak point inside this huge conglomerate and SIKUR Messenger fits great on it.

References

1. https://www.bleepingcomputer.com/news/security/fbi-warns-of-cyber-attacks-targeting-us-automotive-industry/#.XdvDkblyqbk.linkedin
2. https://www.freep.com/story/money/cars/chrysler/2019/12/18/dodge-chrysler-fca-peugeot-merger/2687303001/
3. https://edition.cnn.com/2019/11/20/politics/fbi-us-auto-industry-hackers/index.html