AIRBUS CYBERSECURITY 2019 PREDICTIONS

Markus Braendle
Head of CyberSecurity at Airbus CyberSecurity

AIRBUS CYBERSECURITY

01.

Extortion attacks on OT and IIoT infrastructure

Prediction: Critical infrastructure will be disrupted by a major extortion attack

We've already seen extortion-driven attacks on infrastructure such as cities and ports, which history suggests will continue and spread to energy and transport infrastructure. With the introduction of Industrial Internet of Things (IIoT), manufacturing industry will become a new target. Professional cybercrime is increasingly driven by the simple psychology of extortion, while the almost limitless potential targets are simply a means to a financial end. During 2019, one of these attacks will finally hit home somewhere in the world, causing memorable disruption.

"We expect for 2019 IIoT devices will become a major target for cyber-attackers, especially in the manufacturing industry. The trend with Industry 4.0 to use IIoT technology for real-time data collection of production processes will generate a benefit but also produce an additional risk due to the still low maturity of the cyber security protection of IIoT devices."

said **Head of Airbus CyberSecurity, Markus Braendle.**

02.

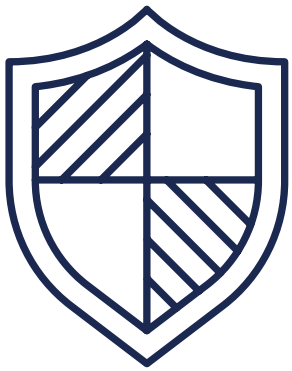
AI's use in malware

Prediction: AI-based malware will 'escape' beyond an intended target with devastating consequences

A malware developer applying Machine Learning (ML) targeting and/or self-propagation could create a strain so capable that if might 'escaped' beyond its intended targets, causing massive collateral damage. The use of AI in such an event will likely increase the fallout beyond that seen with Stuxnet, Mirai and NotPetya. In addition, ML will be used in a real world cyberattack to automate manual hacking techniques usually only associated with APT threats for the first time. Balancing this, Security Operations Centres (SOCs) will start using AI and ML algorithms as a way of plugging the Cyber Security skills gap. The Security Analyst role will have to adjust to accommodate these new artificial colleagues.

"Open Source Machine Learning Libraries/Frameworks such as TensorFlow and Pytorch are making these sophisticated techniques ever more accessible,"

said **Head of Airbus CyberSecurity, Markus Braendle.**



03.

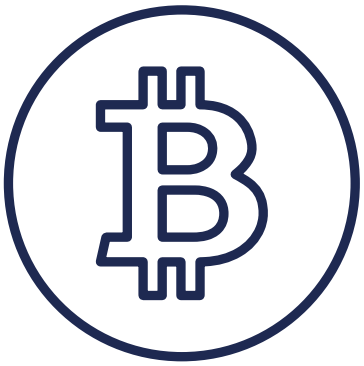
Cryptocurrency regulation

Prediction: Regulators will lose patience with cryptocurrencies

Blockchains are a short-term risk because the technology is immature and heavily tied to the fate of cryptocurrencies. This needs to mature if the technology is to succeed in areas such as supply chain security. As cryptocurrencies become mainstream, the worry of attacks on blockchain currency for geo-political gain will rise. For this reason, they will face increased controls to mitigate economic risk as they traded more in conventional markets. More generally, confidence in blockchain will take a knock as worries over security problems with cryptocurrencies increase and with a realisation that blockchain is not a panacea.

"The security concerns that have emerged with some crypto-currencies are likely to lead to closer attention from the financial authorities and stricter regulation as they become more mainstream,"

said **Head of Airbus CyberSecurity, Markus Braendle.**



04.

World's first cybersecurity treaty

Prediction: Two cyber-powers will start negotiations to agree the world's first cybersecurity treaty

There is a growing danger that people will get hurt because of a deliberate or inadvertent attack on critical infrastructure such as power stations and hospitals. Ideas to address these dangers have included Microsoft's suggestion of a digital Geneva Convention with an independent NGO, the Global Cyber Attribution Consortium, to monitor compliance. Although this and other UN initiatives could take years to come to fruition, the balance of risks v rewards are steadily tipping towards a system of rules for at least some nations, especially if this had geo-political advantages mirrored in other economic and military ties. A formal cybersecurity treaty of this kind would rest as much on its political and symbolic capital as its technical detail.

"States needs to advocate the need for cyber cooperation instead of cyber-warfare. Indeed, states have an obligation to work towards such as treaty to make this happen to prevent harmful cyber-attack. 2019 could be the year for such an agreement for neighbouring countries,"

said **Head of Airbus CyberSecurity, Markus Braendle.**

05.

Ransom ban

Prediction: A local government somewhere will ban public-sector ransomeware payments

It has become commonplace for public sector organisations to pay ransom payments when critical systems are hijacked by extortion attackers. This has always been controversial and the rules governing it's the legality is complex even in developed legal systems. Now, the price of this short-termism is starting to dawn on governments. Payment risks financing new attacks, offers no guarantee against repeat episodes, while the ransom sums themselves have increased tenfold. Attackers are also moving towards ransoming critical infrastructure, a dangerous development. Banning ransom payments might deter extortion attacks and encourage investment in the sort of security designed to avoid them happening.

"With the ransom sums being demanded rising dramatically in 2018, a growing number of organisations have been paying up. This isn't sustainable, especially in the public sector – eventually voters' patience might snap,"

said **Head of Airbus CyberSecurity, Markus Braendle.**

Conclusion

In conclusion **Head of Airbus CyberSecurity, Markus Braendle,** stated:

“Our predictions for 2019 are an indication of how the world has become complex and unpredictable. Coping requires having partners onboard whom you absolutely trust.”

“At Airbus Cybersecurity, we’re also seeing a trend for organisations to move away from simply building high walls to focus more investment on forward intelligence, real-time detection and response.”

Airbus CyberSecurity’s recommendations:

1. IT and OT cybersecurity must be assessed at the board level and managed as part of an organisation’s corporate risk-management.

2. Too many organisations get distracted by shiny boxes - businesses must always find a balance between spending on response and training as well as detection.

3. If you want to be successful, you need to build multi-skilled teams able to collaborate internally as well as externally. No single department or organisation can do this alone.

AIRBUS CYBERSECURITY

For more information please visit

www.airbus-cyber-security.com