Cyber Security expert shares critical concerns on recent OPTUS hack that no one is talking about

An article published by The Australian Broadcasting Commission (ABC) news calling for better protection of customers and their personal data is valid but it is also possibly extremely dangerous says leading cybersecurity expert David Barnes.

MELBOURNE, Australia – Monday 26, 2022

After the most recent compromise at Optus of an estimated 100,000 customer records, the article published online by the ABC dated September 23rd calls for more powers for the privacy regulator. This call could in fact have the opposite desired outcome which is to enable organisations to be held to account for such breaches when in fact it is these types of legislation that empowers the cyber-criminal underworld. Put simply the higher the penalty the higher the ransom.

Research shows that little to none of the ASX 200 companies and Australia's largest companies have put sufficient 'locks on the doors' of their networks to prevent email breaches or sinister attempts using known third party domains. Optus is no exception, in fact the Chief Security Officer (CSO) of Optus in a 2021 meeting with cyber insurance experts pulled out of the meeting within the first 20 minutes citing he was uncomfortable with the metrics being presented on Optus email vulnerabilities. In fairness, the Optus CSO is like most others and naive to the realities relating to email and domain cybersecurity.

Evidence will show that instead of closing the 300,000 vulnerabilities, Optus tried to mitigate just one risk but then opened up 18 million trillion more, literally. Robust standards are what is missing in an often arrogant and ignorant world of corporate IT executives and regulators. CSOs and IT managers are still listening to 25-year-old cybersecurity methodologies peddled by large IT firms. In 25 years, the problem is now worse than ever, as more personal data is held electronically and reactive cybersecurity measures are severely outdated.

"There is a chasm between IT, business logic and understanding email and cyber security in the todays world" says David Barnes, Zulu Labs Inc CEO, Australia's homegrown world leader in cyber email and domain security.

But the lack of cohesive knowledge and experience goes deeper than just knowledge transfer. It can be linked to naive Government intervention that has created a safe and more lucrative World for cyber criminals.

The research shared in a 2021 paper authored by David Barnes for the insurance industry and the previous Australian Federal Government, demonstrated a fundamental link between increased privacy protection after the implementation of the GDPR (the European Union's privacy legislation) and increased cyber-criminal activity that authorities, like the Australian Federal Police, are powerless to investigate.

Redacted ownership records guised for p*rivacy reasons* and the use of proxy domain name system (DNS) services make it nearly impossible for authorities to investigate cyber criminal's and their illegal online activities. When records are proxied or redacted, court orders to discover illegal activities such as online gaming sites targeting Australians often reveal nefarious actors are not operated in jurisdictions such as Curacao or other similar destinations, where warrants cannot be served. This takes up enormous resources including time and money which makes efforts by the AFP fruitless.

David Barnes says "*After the court case against the IOOF subsidiary we created a sampled index of their licensees with 0/30 taking basic necessary steps to secure their email and domain borders. This information will be passed on to ASIC. Indeed, until this proactive cybersecurity measure is implemented for every organisation, every domain operator is a sitting duck.*"

ENDS

Media Enquiries

Ranil Rajapaksha

media@zululabs.com