OPM and AT&T Security, Risky as Vegas Style Slots

Have you noticed? The largest US Based Cyber-Security Hacks in recent years including this week's OPM breach have all come up on the "vastly over-rated" and under secured network of AT&T?

According to sources close to investigations, "it's just a matter of fact." Not much satisfaction though to the "infected or affected" but here's what AT&T says: http://www.csid.com/attcustomercare/

By now you may have heard that China vs. U.S. isn't working out well for the US Government and yesterday announced that another Four Million (plus) government workers have had their identity stolen. This is the third (3rd) time on the Obama watch that a massive breach has happened and still… no word from the White House, no action, only confusion but what else is new there?

On February 12, 2015 on LinkedIn, the vary topic of State Sponsored Attacks was being dissected, analyzed and brought to the attention of anyone willing to listen. Earlier, the U.S. Office of Personnel Management (OPM) had been compromised (in December 2014) and the the security breach wasn't found until a software upgrade failed to identify older vulnerabilities. Unfortunately – it seems that our government and AT&T still have their hands firmly planted over their ears!

But it's never too late, right! Just imagine what could be done. Moving from a reactive to proactive posture and from an defensive to an offensive mentality as was discussed last month in the May edition of CIO Review Magazine. For example, freezing certain Chinese financial interests under our control may seem overzealous; however, anything short of that suggests that we all just accept the status-quo and remind ourselves that our once great nation is being run by the most corrupt, spineless and pathetic group of Anti-American Constitutional supporters since the 2nd War. Can you hear me now? (oh, that was a Verizon plug, sorry!)

Let me first say that we (US ProTech as a company) are a direct partner of CenturyLink and many others which means – by the nature of this article – that if you're concerned about your network and security, we can provide you a no-cost, no-obligation proposal to replace your AT&T circuits (that's my 10 second promo). And get this… when working with US ProTech, you actually pay less than if you were to buy direct. So, thanks for

reading further and for allowing US ProTech the opportunity to earn your business. That said – let's get to the good stuff!

AT&T's network looks more and more like Las Vegas style slot machines… only when it comes to US Government networks – they play like the loosest slots in town. It seems that everybody has their number and if you're China and ready to "play the slots" against the US, they have a real advantage between unsecured AT&T network architecture and governmental over confidence, as we witness security breach after security breach. Maybe it's time that we have a look under-the-hood of AT&T. It would be strange to think that we might find a special Honey-Pot failure or a few unlocked doors, right?

Never fear, big brother is here! The following excerpt is taken directly from a US Military communication making it's rounds on Friday June 5th. "Security Advisory - Information About the Recent Cyber security Incident (below) and Necessary action to take if YOU SUSPECT that your information has been compromised" (*Which it has*).

Here's part of the official OPM Memorandum: "The U.S. Office of Personnel Management (OPM) recently became aware of a cyber-security incident affecting its systems and data that may have compromised the personal information of current and former Federal employees."

Within the last year, OPM has undertaken an aggressive effort to update its cyber security posture, adding numerous tools and capabilities to its networks. As a result, in April 2015, OPM became aware of the incident affecting its information technology (IT) systems and data that predated the adoption of these security controls.

Since the incident was identified, OPM has partnered with the U.S. Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT), and the Federal Bureau of Investigation to determine the impact to Federal personnel. And OPM immediately implemented additional security measures to protect the sensitive information it manages.

Beginning June 8 and continuing through June 19, OPM will be sending notifications to approximately 4 million individuals whose Personally Identifiable Information was potentially compromised in this incident. The email will come from opmcio@csid.com and it will contain information regarding credit monitoring and identity theft protection services being provided to those Federal employees impacted by the data breach. In the event OPM does not have an email address for the individual on file, a standard letter will be sent via the U.S. Postal Service.

In order to mitigate the risk of fraud and identity theft, OPM is offering affected individuals….. (more). Please sign up at www.USProTech.com and request the full article to get the remaining 2 pages of information if interested.

See the following links for additional information:

https://www.identitytheft.gov/

http://www.consumer.ftc.gov/articles/pdf-0088-ftc-memo-law-enforcement.pdf

Thanks for reading and since you've come this far I'd like to say this: The Government seems dead set on learning, taking and stealing whenever it feels justified. What country wouldn't be pissed off at the US when we see the strong arm of the US Government pressuring US Manufactures to build in customized Back-Doors into their hardware being shipped to specific foreign nations? I ask this because it's a fact - and now these businesses are being black-Listed by those same countries - never to do business with them again. And that my friend is simply a shame. Shame on you - NSA! And can we get a Wake-Up Call for AT&T?

Best Regards,

Jonathan Goetsch

CEO

US ProTech