What Star Wars Teaches Us About BYOD and IT Security

At the SecTor security conference, the head of Security Engineering for Check Point explains how modern IT risks such as APTs and BYOD relate to the mythology of Star Wars.

By Sean Michael Kerner | October 04, 2012

TORONTO - For the last 35 years, Star Wars has been the cornerstone of mainstream and geek cultural awareness. While Star Wars is a piece of dramatic fiction, many have found inspiration and solace in it that can apply to the everyday real world. According to Kellman Meghu, head of Security Engineering for Check Point Technologies, Star Wars isn't just entertainment; it's also a case study in data security.

Meghu was the lunchtime keynote speaker at the SecTor security conference, where he stepped outside the box of Star Wars fandom to give a new security opinion on George Lucas' Star Wars: A New Hope.

As a security professional speaking to an audience of security professionals, terms like CSO (Chief Security Officer), APT (Advanced Persistent Threat) and BYOD (Bring Your Own Device) are well known. Those terms are not, however, typically part of the Star Wars lexicon. Meghu's talk was officially titled, "How Not to Do Security: Lessons Learned from the Galactic Empire," and it was riddled with modern IT security acronyms, terms and analysis.

While on the surface, Star Wars appears to be a film about the battle of good vs. evil, Meghu framed the movie as a response to a data loss incident. The Empire lost sensitive data that detailed industrial secrets about its new technology (The Death Star), and that's where Meghu's analysis begins. He sees Darth Vader as the CSO of the Galactic Empire. In a typical enterprise network, it would fall on the CSO to assemble the security team after a data loss incident.

Using clips from the film, Meghu showed the response (the first scene when an Imperial Star Destroyer boards Princess Leia's consular ship). Rather than viewing that as a boarding exercise, Meghu noted that the CSO had traced the data down.

The challenge though, was that the data had been put on a removable device, which is a challenge that enterprises big and small face everyday. The BYOD trend in modern enterprises means that employees bring in their own devices and USB keys can potentially be significant threats. In the Star Wars example, the BYOD is the droid R2-D2 and the 'D' in BYOD stands for droid.

"The data was not just put on removable media, it was put on a fully mobile platform," Meghu said.

When R2-D2 and his peer C3P0 escape in a life pod, the Empire monitored the data's exit but did not fire on them. Meghu noted that it's clear the Empire had a 'monitor-only' policy in place. The monitor only policy is one that plagues many IT security deployments, where there is monitoring in place but no actions are taken.

That said, in any enterprise network, monitoring of all events is key. That's what happened to the Empire: They had logs and they were able to trace down where the data loss occurred and where it went.

The final attack on the Death Star was analyzed by Meghu as the delivery of an Advanced Persistent Threat (APT).

Lessons Learned

In Meghu's view, Star Wars provides some key takeaways for enterprise IT security. There was a data loss incident and a security policy implemented by the CSO, Darth Vader.

"The Galactic Empire knew what data was important, they monitored,logged and reported on access and they responded to threats," Meghu said.

That said, the larger issue and the key flaw was a failure in the BYOD policy. In the Empire's network, apparently anyone could plug in a droid and access whatever they wanted. Meghu suggested that R2-D2 was just a giant USB stick and there should always be a policy in place for removable media. He also argued that the Galactic Empire did not properly encrypt sensitive data and they had a weak handling policy.

Meghu said a correct security policy for both the Empire and enterprise IT is all about role-based access control. Access should only be given to the droids and people that need access to a given system and it should be locked down for everyone else.

In the final analysis, what Star Wars teaches is that it is important to protect all the important data that you have with core access control.

"For all the money that we spend on security infrastructure, unfortunately most of the time it's the little things that get us," Meghu said. "It's as simple as something just walking out the door, with the wrong piece of data at the wrong time."

Sean Michael Kerner is a senior editor at eSecurity Planet and InternetNews.com, the news service of the IT Business Edge Network. Follow him on Twitter @TechJournalist.