LBMC Information Security Cybersecurity Sense Podcast Show Notes
Author: Bill Dean
Episode: 9
Date: October 3, 2017

Kaspersky vs the U.S. Government

Softpedia.com: Kaspersky Antivirus Banned by Best Buy Due to Spying Concerns

- Full story link: http://news.softpedia.com/news/kaspersky-antivirus-banned-by-best-buy-due-to-spying-concerns-517683.shtml
- The United States government is accusing Kaspersky of hiding backdoors into its software to help Russia spy on high-profile users.
- The FBI has been concerned about Kaspersky for as long as I can remember and are reported to have been approaching private sector companies to ban and remove Kaspersky products from their systems.
- This was after the U.S. government decided to remove Kaspersky from the approved vendor list, citing spying concerns.
- I recall even seeing an interview with the FBI on the nightly news recently, raising the alarm about Kaspersky.
- We even have Senators getting involved in the accusations, stating that six top intelligence officials that included the head of the CIA and FBI voted against the use of Kaspersky.
- I am not an expert on diplomacy but must think this isn't going to help relations between the countries.
- Best Buy is willing to replace recently-purchased licenses of Kaspersky with other security products in the next 45 days.

Takeaways

- To many, it feels like the U.S. government is trying to make information security decisions for us.
- I don't have an opinion either way on the decision, but we must assume that they have some sort of intelligence for this war against Kaspersky.
- While it seems a bit extreme, this isn't the first time the U.S. government has publicly expressed security concerns related to technology companies based in countries of concern from a cybersecurity perspective.
- In 2011, the U.S. House Intelligence Committee reported that Huawei, a Chinese telecom giant "can't be trusted to install phone and data networks because they could pose a threat to U.S. national security" and that they could not be trusted "to be free of foreign state influence." Of course, China is the foreign state of concern.
- This claim was followed up by a *60 Minutes* episode dedicated to the potential national security concern.
- One issue for one of my clients at the time was that they had a Huawei storage system, and they received government funding. They received a letter from Congress stating

concern, and we worked with them to monitor the system for communications of concern and air-gapped it from any internet communications in or out. If maintenance needed to occur, a technician would have to come on-site.

- Then, in 2014, IBM sold their PC business to Lenovo, which is based in China. Same concerns again, as many government agencies were buying PCs and desktops from IBM.
- We all must admit that concerns of cyberespionage from the Chinese government, while not directly related to Huwei or Lenovo, have been warranted.
- So, what do you do if you have Kaspersky has your AV? I have spoken to a client in the energy sector who uses Kaspersky, and they are getting a lot of pressure to replace it.
- For those of you in the private sector, the choice is ultimately yours.
- The good news is that traditional AV is pretty much a commodity at this point, and Kaspersky does not provide NextGen AV functions, such as endpoint visibility, hunting capabilities, or much of anything outside of signature-based protection.
- There are 40 or more products that will do the same thing, and some are free.
- Microsoft Security Essentials and Windows Defender are viable free options, and Windows Defender on Windows 10 has a new ATP (Advanced Threat Protection) module that has promise-based on the marketing. See link in references below.
- For those who know me, you know that I am not suggesting to stop with AV alone.
- I have been suggesting to take advantage of Microsoft Security Essentials and Windows Defender and then taking the investment that was being made into other products and consider repurposing those funds for an endpoint visibility with Carbon Black with quality threat intelligence feeds.

Bill Dean is a Senior Manager at LBMC Information Security. While involved in various aspects of LBMC's security services, he is also the practice lead for the organization's incident response, forensics, and litigation support practice.

References:

http://news.softpedia.com/news/kaspersky-antivirus-banned-by-best-buy-due-to-spying-concerns-517683.shtml

https://www.cheatsheet.com/business/lenovos-ibm-deal-has-sparked-national-security-concerns.html/

https://www.forbes.com/sites/simonmontlake/2012/10/08/u-s-congress-flags-chinas-huawei-zte-as-security-threats/

https://blogs.windows.com/windowsexperience/2016/03/01/announcing-windows-defender-advanced-threat-protection/