It's Data Privacy Day and not Maple Syrup Day:

Or why Microsoft's 5th Immutable Law of Security rules them all

By

Marc van Kralingen

Marc.vankralingen@Quest.com

I live in Canada and my colleagues in other parts of the world like to give us a hard time about our holidays. I was slow responding to an e-mail last Friday and Tom accused me of being off celebrating Maple Syrup Day, so I gave him a flippant response… but to my chagrin there is a National Maple Syrup Day! https://nationaldaycalendar.com/national-maple-syrup-day-december-17/

Regardless, today is Data Privacy Day and is celebrated the world over to raise awareness and promote privacy and data protection best practices. To do my part to honor this most solemn of occasions, I wanted to talk about something that comes up a lot, namely Check-box Security, and how it relates back to Microsoft's 5th Immutable Law of Data. But first…

Warning: This blog post waxes poetic at times.

Check-box Security and Microsoft's 5th Immutable Law of Security Administration

All too often IT security gets relegated to "**check-box security**". Check-box Security is the characteristic of an organization that adheres to the strict letter of the law for satisfying security controls, often driven by compliance regulations, but ignores the spirit of the requirements and thus falls back onto incomplete and inadequate security controls (Bollinger, et. al., 2015, P:25).

Check-box Security fails to adhere to Microsoft's **5th Immutable Law of Security Administration** which states that "Eternal vigilance is the price of security" (Culp, 2014). Initially written by Scott Culp back in 2000, these Ten Immutable Laws maintained by Microsoft seem to have aged like a fine wine and have only gotten better with time (hey, I warned you in the Summary above). See the references section at the end of this blog post for a link to these Immutable Laws, they make for a fun read and according to Microsoft requires only 14 minutes to get through!

For convenience, Scott Culp's complete list of Immutable Laws of Security are recopied here:

- Law #1: Nobody believes anything bad can happen to them, until it does
- Law #2: Security only works if the secure way also happens to be the easy way
- Law #3: If you don't keep up with security fixes, your network won't be yours for long
- Law #4: It doesn't do much good to install security fixes on a computer that was never secured to begin with
- Law #5: Eternal vigilance is the price of security
- Law #6: There really is someone out there trying to guess your passwords
- Law #7: The most secure network is a well-administered one

- Law #8: The difficulty of defending a network is directly proportional to its complexity
- Law #9: Security isn't about risk avoidance; it's about risk management
- Law #10: Technology is not a panacea

The link I make here between check-box security and Microsoft's 5th Immutable Law I will credit to the Microsoft team. In their great article "Monitoring Active Directory for Signs of Compromise", Math et. al. reference the 2009 Verizon Data Breach in which Verizon found that:

> "*The apparent ineffectiveness of event monitoring and log analysis continues to be somewhat of an enigma. The opportunity for detection is there; investigators noted that 66 percent of victims had sufficient evidence available within their logs to discover the breach had they been more diligent in analyzing such resources.*"

The situation seems to worsen by 2012 as Math et. al. go on to state that:

> "*This lack of monitoring active event logs remains a consistent weakness in many companies' security defense plans. The 2012 Verizon Data Breach report found that even though 85 percent of breaches took several weeks to be noticed, 84 percent of victims had evidence of the breach in their event logs*."

Conclusion

The evidence of breaches is there but isn't acted upon fast enough. Microsoft's 5th Immutable Law of Security, Eternal Vigilance, is not being practiced. Despite the victims having enough evidence within their logs to discover their breaches, they didn't - at least not fast enough. The statistics called out in red above serves as evidence to support the argument for machine learning and user and entity behavior analytics (UEBA) to enhance defense-in-depth strategies. I'll discuss UEBA in a future blog post. In conclusion, if I had to choose one law, I'd choose #5 to rule them all: "*Eternal vigilance is the price of security*".

Thanks and Happy Data Privacy Day,

MvK

Related posts

Winder, David. 2019. "11 Expert Takes On Data Privacy Day 2019 You Need To Read". https://www.forbes.com/sites/daveywinder/2019/01/27/11-expert-takes-on-data-privacy-day-2019-you-need-to-read/#5f6ff34375a2

References

Bollinger, Jeff. Brandon Enright, and Matthew Valites. 2015. "Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan". O'Reilly Media Inc. California.

Culp, Scott. 2014. "10 Immutable Laws of Security Administration". Retrieved from: https://docs.microsoft.com/en-us/previous-versions//cc722488(v=technet.10)

Math, Bill. et. al. 2017. “Monitoring Active Directory for Signs of Compromise”. Retrieved from: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise