Security, Fear, Uncertainty, and Doubt

By *Roy Schestowitz*
Created *20/07/2021 - 9:43pm*
Submitted by Roy Schestowitz on Tuesday 20th of July 2021 09:43:36 PM Filed under Security [1]

- **How IBM i Fits Into a Zero-Trust Security Framework [2] [Ed: Authored by IBM shill funded by IBM]**

  One of the hot new trends in cybersecurity these days is the zero-trust security model. Instead of implicitly trusting network traffic behind the firewall, zero-trust demands that traffic have explicit permission to be there. But how does that model work with the strange beast known as IBM i? IT Jungle recently sat down with PJ Kirner, the CTO and co-founder of zero-trust software provider Illumio, to find out.

  Illumio is an eight-year-old venture-backed startup based in Sunnyvale, California, that is working in the field of zero-trust security. It develops an offering, called Illumio Core, that allows companies to begin implementing the zero-trust security model in their own data centers.

  It?s a fairly radical shift in philosophy, Kirner says. ?There?s a mentality change from ?I trust everything? to . . . ?I need a policy enforcement point of some sort everywhere, not just in the one place at the boundary of two things,'? he says.

  When fully built out, an IT estate with an active zero-trust security model will resemble a party where only invited guests are allowed in. Building from a whitelist, or ?allow list,? is starkly different than starting with a blacklist, or an ?exclude list,? Kirner says. ?If you start by saying just these two things are not allowed to talk, well, that?s a whole bunch of implicit trust around everything else,? he says.

Illumio, which recently added support for IBM i systems, begins every zero-trust security engagement by making a map of network traffic behind the firewall. Illumio develops software that does this mapping, which can be quite illuminating in its own right.

- **New Windows 10 vulnerability allows anyone to get admin privileges** **[3]**

- **The virus rears its ugly head....** **[4]**

  There is a virus going around. We thought we were winning the battle against it, but powerful forces and events have allowed it to raise its ugly head and cause unforeseen additional hardship.
  People thought that it was not so bad, they did not listen to reason and take the precautionary measures necessary to protect themselves. In letting down their guard they were unprepared and unprotected.
  After months of machines being turned off, software licenses (with their expiration dates never ?dormant?) are up for renewal.
  Many companies, educational institutions and public buildings (like libraries) are turning on their Wintel PCs for the first time in over a year and finding that they need to renew their licenses, not only for what is called an operating system on their computer, but also for many of the closed source, proprietary add-on software packages that owners purchased in a wild attempt to make their hardware somewhat useful.

  [...]

  This variant is called ?Windows 11?, and the creator of it seems to be unable to tell you how much havoc it will create for you. Does it run on your otherwise great hardware? You have a decent processor, a lot of RAM, and you bought it just two or three years ago?.but it might not run Windows 11.

- **UK.gov's Huawei watchdog says firm made 'no overall improvement' on firmware security but won't say why** **[5]**

  Huawei has made "no overall improvement" in software engineering processes for its UK telecoms equipment's firmware, its GCHQ overseers have warned.

  The Huawei Cyber Security Evaluation Cell (HCSEC) oversight board's annual report for 2020 was noticeably less critical than in previous years ? but still says Huawei is dragging its feet in key areas.

- **Northern Train's ticketing system out to lunch as ransomware attack shuts down servers** **[6]**

Publicly owned rail operator Northern Trains has an excuse somewhat more technical than "leaves on the line" for its latest service disruption: a ransomware attack that has left its self-service ticketing booths out for the count.

"Last week we experienced technical difficulties with our self-service ticket machines, which meant all have had to be taken offline," a spokesperson for Northern Trains confirmed to the The Register.

- **Fortinet's security appliances hit by remote code execution vulnerability [7]**

  Security appliance slinger Fortinet has warned of a critical vulnerability in its products that can be exploited to allow unauthenticated attackers full control over the target system - providing a particular daemon is enabled.

  The vulnerability, discovered by Orange Group security researcher Cyrille Chatras and sent to Fortinet privately for responsible disclosure, lies in the FortiManager and FortiAnalyzer software running atop selected models in the company's FortiGate security appliance family. Should a particular daemon be enabled, the company admitted, a remote attacker can gain full control.

- **Romanian Linux Cryptojacking Cybercriminals Spotted [8] [Ed: This is classic FUD as it's not a Linux issue but a weak password issue]**

  Since at least 2020, an active threat organization based in Romania has been running a cryptojacking operation against Linux-based machines using the Golang-based SSH brute force, according to The Hacker News. The campaign's objective is to infect Linux systems with Monero mining applications.

Security

Source URL: http://www.tuxmachines.org/node/153610

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://www.itjungle.com/2021/07/19/how-ibm-i-fits-into-a-zero-trust-security-framework/
[3] https://www.bleepingcomputer.com/news/microsoft/new-windows-10-vulnerability-allows-anyone-to-get-admin-privileges/
[4] https://www.linux-magazine.com/Online/Blogs/Paw-Prints-Writings-of-the-maddog/The-virus-rears-its-ugly-head
[5] https://www.theregister.com/2021/07/20/huawei_hcsec_oversight_report_muted_criticism/
[6] https://www.theregister.com/2021/07/20/northern_trains_ticketing_system/
[7] https://www.theregister.com/2021/07/20/fortinet_rce/
[8] https://news.softpedia.com/news/romanian-linux-cryptojacking-cybercriminals-spotted-533536.shtml