Rating Risk in Your Enterprise

Dean Webb

Security Pro

☺

So I started a new job…

- Orientation made me watch my company’s CEO keynote
- Also a presentation by some Harvard professor…

- They were so compelling, I watched them both several times and I bought the professor’s book, The Devil Never Sleeps
- Both dealt with the concept of evaluating risks…

Techies vs Executives

- Two groups that see different things when they look at assets
- The nature of their roles requires that difference
- One will want a new firewall because the old one has technical issues, is hard to work with, and is prone to outages
- The other will want a new firewall because it offers enhancements that should streamline line of business functions, reducing overall costs.
- *They are not the same!*

What do the techies know about a device?

- Addresses: IP, MAC, VIP, subnet mask, gateway
- Components: CPU, RAM, Storage, BIOS version
- Software: OS, version, installed apps, running services
- Physical info: Rack location, power consumption, cooling needs, Hardware manufacturer, KMV connection
- Org info: who is in charge of it, what departments touch it, who is responsible for maintenance and upgrades… and billing…

…and billing…

- How much is the device worth?
  - Data stored on it
  - Function(s) performed on it
  - Process connections in workflows
  - Criticality to line of business functions
- If that device went offline, how much would it cost the business?
- If that device were compromised and its data impacted, how much would it cost the business?
- What is that device *actually worth?*

Why Is Device Value Important?

- What makes the better value statement?
  - “We just patched 357 vulnerabilities in the last hour!”
  - “We reduced the potential losses due vulnerable code by $100,000… in the last hour!”
- Executives can best understand security benefits in terms of money and/or work-hours saved.
- Device values allow security efforts to be translated into monetary terms.

How do we capture data on device value?

- Executive/management exercise
- Critical path analysis
    - Process flow: server to server
    - Communication flow: server to switch to router to switch to server
    - Intermediate devices share in the value proposition
- Organizational intelligence
    - “If *that* switch goes down, we are all in a world of hurt!”
    - “These network ranges are *off limits* to our team!”
    - “That’s the trading floor. *Don’t touch it!*”

Capture values, then assess risks

- All devices, even sensitive ones, need risk assessment
  - Zero-day vulnerabilities
  - Lacking critical patches
  - Risky configuration options
  - End-of-Service/End-of-Life devices/applications
  - Unneeded services/applications installed/running
  - Vulnerabilities in communication chain
- Chance that one or more of these contributes to a failure, multiplied by value, equals dollar amount at risk to enterprise

Executive decisions…

- Once we know $$$ at risk on a given asset, an executive can…
    - Appreciate remediation that reduces $$$ risk
    - Understand costs where remediation is not currently possible
    - Prioritize security and maintenance projects and processes
- Reducing risk $$$ should be tracked by IT/Security teams
    - Justify spend on tools, staff
    - Change perception:
        - NOT “cost center”
        - BECOME “cost reduction center”

Ideally…

- Security teams would look beyond criticality scores for risk
- Ease of exploitation is a factor
- As is ease of remediation
- Zero-trust measures in place, especially with identities
  - Human
  - Service
  - API
  - And watch out how AI uses API exploits to do its job…

Disclaimer Time!

- My new job is with Qualys.
- Qualys offers a platform that will check devices for issues and then put a $$$ amount on those, based on asset value.
- Back to being vendor-neutral… but I *do* want to address what I see as an ideal situation for an enterprise…