The Need for IT Operations Agility: Lessons of WannaCry

There is little doubt that the news of ransomware like the recent outbreak of the WannaCry (aka Wcry, WannaCrypt) taking hold in critical infrastructure hits home with every IT professional. The list of affected clients of any ransomware or critical vulnerability is made even more frightening when it means the shutting down of services which could literally affect people's health like the NHS is experiencing.

Would it be any different if it were a small hardware chain? What if it was a bank? What if it was your bank, and your money was now inaccessible because of it? The problem just became very real when you thought about that, didn't it?

Know Your (Agile) Enemy

Organizations are struggling with the concept of more rapid delivery of services. We often hear that the greatest enemy of many products is status quo. It becomes even more challenging when we have bad actors who are successfully adopting practices to deliver faster and to iterate continuously. We aren't talking Lorenzo Lamas and Jean Claude Van Damme kind of bad actors, but the kind who will lock down hospital IT infrastructure putting lives at risk in search of ransom.

While I'm writing this, the WannaCry ransomware has already evolved and morphed into something more resilient to the protections that we had thought could prevent it from spreading or taking hold in the first place. We don't know who originally wrote the ransomware but we do know that in the time that we have been watching it that it has been getting stronger. As quickly as we thought we were fighting it off by reducing the attack surface,

The Risks of Moving Slowly

Larger organizations are often fighting the idea of risks of moving quickly with things like patching and version updates across their infrastructure. There are plenty of stories about an operating system patch or some server firmware that was implemented on the heels of its release to find out that it took down systems or impacted them negatively in one way or another. We don't count or remember the hundred or thousands of patches that went well, but we sure do remember the ones that went wrong. Especially when they make the news.

This is where we face a conundrum. Many believe that having a conservative approach to deploying patches and updates is the safer way to go. Those folks view the risk of deploying an errant patch as the greater worry versus the risk of having a vulnerability exposed to a bad actor. We sometimes hear that because it's in the confines of a private data center with a firewall at the ingress, that the attack surface is reduced. That's like saying there are armor piercing bullets, but we just hope that nobody who comes after us has them.

Hope is not a strategy. That's more than just a witty statement. That's a fact.

Becoming and Agile IT Operations Team

Being agile on the IT operations side of things isn't about daily standups. it's about real agile practices including test-drive infrastructure and embracing platforms and practices that let us

confidently adopt patches and software at a faster rate. A few key factors to think about include:

- Version Control for your infrastructure environment
- Snapshots, backups, and overall Business Continuity protections
- Automation and orchestration for continuous configuration management
- Automation and orchestration at all layers of the stack

There will be an onslaught of vendors using the WannaCry as part of their pitch to help drive the value of their protection products up. They are not wrong in leveraging this opportunity. The reality is that we have been riding the wave of using hope as a strategy. When it works, we feel comfortable. When it fails, there is nobody to blame except for those of us who have accepted moving slowly as an acceptable risk.

Having a snapshot, restore point, or some quickly accessible clone of a system will be a saving grace in the event of infection or data loss. There are practices needed to be wrapped around it. The tool is not the solution, but it enables us to create the methods to use the tool as a full solution.

Automation and orchestration are needed at every layer. Not just for putting infrastructure and applications out to begin with, but for continuous configuration management. There is no way that we can fight off vulnerabilities using practices that require human intervention throughout the remediation process. The more we automate, the more we can build recovery procedures and practices to enable clean rollbacks in the event of a bad patch as well as a bad actor.

Adapting IT Infrastructure to be Disposable

It’s my firm belief that we should have disposable infrastructure wherever possible. That also means we have to enable operations practices which mean we can lose portions of the infrastructure either by accident, incident, or on purpose, with minimal effect on the continuation of production services. These disposable IT assets (software and hardware) enable us to create a full stack, automated infrastructure, and to protect and provide resilience with a high level of safety.

We all hope that we won’t be on the wrong side of a vulnerability. Having experienced it myself, I changed the way that I approach every aspect of IT infrastructure. From the hardware to the application layers, we have the ability to protect against such vulnerabilities. Small changes can have big effects. Now is always the time to adapt to prepare for it. Don’t be caught out when we know what the risks are.