Pandemic Response vs. Cybersecurity Best Practices

Over the past few months, we've all witnessed the unfolding of the coronavirus pandemic. We've watched closely as our local, state and federal leaders work to contain its spread in order to save lives. In the cybersecurity realm, observations have been made as to how similar responding to a pandemic is to following best practices for cybersecurity.

In a **PANDEMIC,** the ultimate goal is to contain the spread of the virus while researchers work feverishly to come up with a vaccine. In **CYBERSECURITY**, the ultimate goal is to contain the spread of the virus while incident response teams work feverishly to get remediation efforts in place to harden the network.

During a **PANDEMIC**, the sick are isolated. For **CYBERSECURITY,** infected systems are locked down with anti-malware tools.

During a **PANDEMIC,** borders are closed and geographic quarantines are put in place. In **CYBERSECURITY,** "borders" are closed by implementing network segmentation in the firewall.

During a **PANDEMIC**, the past movements of infected people are looked at in order to notify others the sick may have been in contact with. For **CYBERSECURITY**, we use logging and monitoring tools to track where the virus has been.

During a **PANDEMIC**, stay at home orders are issued with restrictions that only allow travel for essential needs. Some businesses have checkpoints in place like checking everyone's temperature to weed out people with symptoms before they enter the building. In **CYBERSECURITY,** we monitor and analyze on-wire traffic in order to identify and filter out threats.

During a **PANDEMIC**, criteria is established to help healthcare professionals prioritize which patients to treat first. For example hospitalizing the high risk and most vulnerable patients first and asking healthier individuals to self-quarantine at home. In **CYBERSECURITY**, we deploy asset management tools so we know what we have in our inventory in order to help us prioritize the most vulnerable and critical systems.

"Every second matters when a threat is looming and impacting your network," says Ray Panfil, a Security Analyst and Advisor at RAVENii. "It is vital to your business to plan, prepare and practice for cyber attacks."

Panfil says your plan should include having the right security tools deployed that are monitoring your network and giving you intelligence into what's happening.

"Information is key. We need security tools that can help us identify what threats are out there, what they look like and what systems they are targeting," Panfil said. "You'll be in a better position to fight off viruses with the right tools in place; including documentation for how you use those tools and security policies to provide you with guidance and guidelines."

In conclusion, whether it's a global health pandemic or a cyber threat to your environment, having a plan to follow with the right tools and processes in place can save precious time in saving what's most critical and important to you.

As always, the RAVENii team is here to help you plan, prepare and practice.

Stay safe and be well!

RAVENii
CYBER SECURITY

April 23, 2020