A tale of two pandemics - What cybersecurity can learn from microbiology

2020 will be remembered as a gloomy year. As fate would have it, the world suffered the worst viral and cyber pandemics in history simultaneously. As the new COVID-19 started to kill millions of people across the world, a breach on IT firm SolarWinds (also known as Solorigate) started a supply-chain attack of an unprecedented magnitude, affecting thousands of organisations, including the Pentagon, the White House, the US army, US departments of Treasury, Commerce and Energy, IT giants like Microsoft, Cisco, Deloitte, Intel…

Temps de lecture : minute

---

3 February 2021

With both pandemics still ongoing, we don't yet know the full extent of the damages. But we can look at the initial responses to both crises and start to learn from them.

Managing viral pandemics

Born in the 16th century with the theory of contagious diseases, microbiology witnessed a golden age in the late 1800s and early 1900s. For the next hundred years, scientists would use data, experiments and vaccines to successfully interrupt the unfolding of microorganisms, chains of contamination and epidemics.

> *"Chance only favours the prepared mind" — Louis*

> *Pasteur*

When COVID-19 first made the news, scientists knew exactly what were the first measures to take to stop the chain of contaminations. Almost overnight travels were halted, borders were shut, social gatherings were restricted and half the world went into lockdown. People were asked to stay home, social distance, wear masks and wash hands.

From the early months, we saw that wherever rules were strictly enforced like in New Zealand, there was a successful decline in the epidemic. On the other hand, social gatherings were virus spreading grounds; some even turned into super-spreader events, as they started a new chain of infections carrying the virus to new clusters.

Managing cyber pandemics

Cybersecurity on the other hand is a young industry. The first computer virus was created in 1971. But in its short life-span, the world changed dramatically from using pen and paper to doing everything online. In the gold-rush years of going digital, accessibility became the imperative, often relegating cybersecurity to an after-thought.

But as cyber-attacks increased in number, size and impact, cybersecurity spends increased too. Most investments went into detection and remediation, which while preventing many attacks, failed to detect or stop cyber pandemics.

The main difference between the viral and cyber pandemics lies in the approach to risk.

For the last five years, over 80% of data breaches have started with weak, reused and stolen passwords. As the human brain was never meant to

create and remember strong unique passwords, people keep using the same password or password patterns they can remember, which makes them easy to crack using social engineering, brute force, credential stuffing, dictionary attacks, password spraying…

To go around the problem, a first generation of solutions centralised passwords on the cloud, giving people a single password to remember to access all their accounts. But what was convenient for users was also convenient for hackers. From one breach, you risked to lose everything at once.

In microbiology, you can carry a virus and not know it. Many people are asymptomatic yet transmit the new coronavirus. Which is why creating bubbles or restricting group size gatherings makes sense. What not to do is put everyone in the same room: if one person has the virus, others will get infected too.

In cybersecurity, many systems have suffered undetected breaches. That’s why it makes sense to create smaller clusters of data and only open the doors to the data you need. What not to do is centralise all your systems in the same place: if one system is infected, others will get infected too.

Lessons from COVID-19 and the Solorigate

1. Centralising people or systems helps viruses spread faster
Microbiologists already know that. For the cybersecurity community, the Solorigate should be a moment of reckoning where some important questions will have to be answered. Why with much increased cybersecurity spendings did we get not less ransomware and supply-chain attacks, but more? How come the vastest operation of cyber-espionage could go on for almost nine months without anyone seeing it?

2. Decentralise to prevent viruses from spreading To mitigate viral pandemics, ask people to stay home, reduce group sizes, apply social distancing, wear masks and wash hands. With vaccines programmes already started, there is hope we will beat this virus.

To mitigate cyber pandemics, distance all systems, create smaller cluster sizes, protect each system with strong unique passwords and decentralise credentials.

MyCena created a breakthrough concept that helps you do that. Based on the principle that passwords are just keys, people don't need to create, type, memorise or even know them anymore. In a decentralised model, if one system is breached, the others are safe

3. Act fast As viral pandemics kill people and cyber pandemics kill companies, there is a race between the virus and the vaccine, between hackers and cybersecurity teams, to see who will get there first.

For government and company leaders, having access to the solutions or vaccines is just the beginning. Success will be measured by the speed and accuracy of the roll-out. Unfortunately bureaucracy can slow vaccination programmes down in some countries, putting more lives and economic recovery at risk.

To accelerate your systems recovery from cyber-breaches,

MyCena has developed a fast and simple process to roll out the solution to all your systems and employees without change of infrastructure.

Last but not least, noone will ever need to create or memorise a password again.

Despite being a gloomy year, 2020 did teach us something important: humility. As we realise our world is interconnected and that certainty does

not exist, we will pay more attention to keeping our family, our company and our planet safe.

Stay safe in 2021.

This article was originally published on ParlayMe.

Julia O'Toole is the founder CEO @Mycena Security Solutions. *MyCena is a cybersecurity company pioneering a revolutionary concept to stop cyber pandemics and mitigate cyber risks. MyCena helps you distance all systems so that if one system is infected, the others remain safe.*

Article by Julia O'Toole