Unsplash © Tai's Captures

Does your business have the right digital antibodies?

With COVID-19 illustrating how a virus can devastate a country, the parallels with networks and computer systems are clear. Can we apply what we've learnt combating COVID-19 to our digital systems?

The computer virus is often compared to their biological cousins. As the COVID-19 crisis continues, can we compare how the coronavirus spreads and, how we are combating its effects to the digital systems we all rely upon to work and play? Do we need to develop digital antibodies for our networks and connected device?

History tells us that cyberattacks can infect digital systems in much the same way COVID-19 has spread throughout the populations of the world. Zero-day worm attacks operate in a similar way to biological viruses. The recent WannaCry attack exploited vulnerabilities in computer systems. Anti-virus applications could not identify the virus, as these applications had no definitions of the new virus. The parallel with the human immune system that has no antibodies to fight COVID-19 is clear.

Zero-day attacks can also be challenging to identify, as they often lie in wait before they become active. The Stuxnet worm is a good example. The COVID-19 virus similarly attacks with the host being asymptomatic for several days – yet remains infectious.

“COVID-19 does pose a threat to those who are healthy and immune,” says Richard Skellett founder of Digital Anthropology. “The threat is about infecting their loved ones and others who they don’t know. It’s the same as networks, and we might have a very healthy network with all the latest technologies, but that will never stop us being infected or penetrated if an organisation wishes to do that. That is why no security solutions company offers a 100% Guarantee. There is not a guaranteed vaccine a computer can take to stop infection when it’s online.”

Placing cybersecurity within the context of COVID-19 must also consider the human element. Indeed, according to the latest report from The Information Commissioner’s Office (ICO) latest report on data security incident trends ‘non-cyber incidents’ defined as people’s behaviour is putting data at risk.

The UK and the rest of the world remain in a state of flux due to the COVID-19 pandemic. But throughout all industries, this is also proving to be a time of revolution for secure digitisation. Large-scale remote working and social distancing are forcing organisations to re-examine established processes, providing an opportunity for innovation that leads to improved security, efficiency and cost-effectiveness.

The cyber habits of the millions of employees now working from home also needs to managed to avoid widespread cybersecurity issues. The COVID-19 crisis has shown us that social distancing can be useful. In the context of remote working however, the potential threat perimeter moves to workers’ homes with a corresponding lack of security control.

According to CyberArk, 57% of respondents to their survey insecurely save passwords in browsers on their corporate devices, 89% reuse passwords across applications and devices and, 21% admitted that they allow other members of their household to use their corporate devices for activities like schoolwork, gaming and shopping.

While 91% of IT Teams are confident in their ability to secure the new remote workforce, more than half (57%) have not increased their security protocols despite the significant change in the way employees connect to corporate systems and the addition of new productivity applications.

“With the accelerated use of collaboration tools and home networks for professional purposes, best-practice security is struggling to keep pace with the need for convenience which, in turn, is leaving businesses vulnerable,” said Rich Turner, SVP EMEA, CyberArk. “Simultaneously, businesses must constantly review their security policies to ensure employees only have access to the critical data and systems they need to do their work, and no more. Decreasing exposure is critical in the context of an expanded attack surface.”

Read also

The Bored Room: How to turn meetings into powerful tools

Wash your digital hands

To gain an insight into how the work being carried out to combat COVID-19 could be applied to network and system security, Maddyness UK spoke with Alex Dalglish, head of future workplace, SoftwareONE and began by asking can we use what we have learnt combating COVID-19 to innoculate our digital systems?

“A key part of combatting COVID-19 has been enforcing social distancing by staying at home, which has been reflected in the widespread move to remote working,” Dalglish explained. “Businesses supporting this en masse shift have had to ensure that the right technology is in place to do so. However, much like in the fight against COVID-19, knowledge is power, and so businesses need to equip their employees with the understanding of how to use the software at their disposal.

“This can be achieved through Adoption and Change Management (ACM) Services ensuring there is a clear and structured process to an organisation-wide adoption of the new technologies, and online training programmes that cover best practice across the many tools available to support remote working.

“All ACM and training programmes should also encompass compliance and security, teaching employees how to avoid putting themselves and the wider business at risk – similar to adhering to lockdown rules. As homeworking is likely to experience a more permanent shift from ‘trend’ to ‘new normal’ post-pandemic, it’s key that businesses do what they can to get the essential steps right.”

The cloud is very much like a population of people. As we understand more about the transmission of COVID-19 and what practical measures work to combat the virus, will this change how we organise and protect the cloud?

“When it comes to organising and protecting the cloud, businesses can learn several lessons from the transmission of COVID-19. Firstly, visibility is hugely important. Monitoring case numbers and the recent harnessing of contact tracing technology has been crucial in predicting the ‘curve’ of the virus.

“Businesses can mimic this by taking an organised, strategic approach to their cloud usage. By identifying exactly what they are using – as well as where and how much – they can have enough visibility over cloud usage to predict spend and ensure that costs don’t spiral.

“COVID-19 has also required societies to identify which services are ‘essential’ and ‘non-essential’ and prioritise or de-prioritise accordingly; businesses can learn another critical lesson here. It’s likely that many organisations are paying for cloud-based services that – due to circumstances changed by the health crisis – is currently unnecessary, and so can be downsized or scrapped entirely.

“Conversely, other SaaS services – such as Zoom and Microsoft Teams –have been essential in supporting a remote workforce. As many businesses look to make necessary cuts in response to an ambiguous future, reassessing software assets will be key to the continued smooth running of the business and keeping costs low.”

COVID-19 poses little threat to most people with healthy immune systems. If we apply this idea to computer networks, what does a ‘healthy system’ look like?

“There are many components to ensuring a ‘healthy’ network. One key area, which is extremely pertinent given the current crisis, is Shadow IT. When employees turn to systems and processes that are outside of the business’ centralised IT, security and financial risks are created – like ‘free radicals’ threatening the immune system.

“To tackle this and keep the IT environment healthy, businesses should look to train employees on the risks that Shadow IT brings. Organisations should also monitor the environment continuously – much like you’d take the temperature of even a healthy person to spot possible infection, even when asymptomatic.”

Dalglish concluded: “Backup is another crucial component to keeping an IT system healthy – like an IT immune system. A healthy immune system ensures a clear route to recovery. Businesses should mimic this and, rather than leaving data security and backup to chance, put an effective backup strategy in place so that any lost data is easily recoverable. By creating a standardised process for data back up, and enhancing security, businesses can be confident that their data crown jewels are protected, no matter what may come their way.”

Read also

Cyber attacks proving challenging for businesses in 2020

Becoming cyber-COVID prepared

A cyber pandemic can be avoided if businesses understand their threat perimeters and the components that must be fully supported to create a secure environment for their systems and workers.

In their report on tech trends, Accenture note: “Threat actors see ecosystems as an ever-widening attack surface, while most businesses still look at cybersecurity as strictly an individual effort. To respond to this dichotomy, organisations need to amend their approach, incorporating security into the collaborative strategies they have used to create powerful and innovative products and services. They must include growing ecosystem dependencies as part of their own security posture and make security a cardinal component of how they build partnerships. Both are a must for security in a post-digital world.”

As biological systems are always vulnerable to attack, so digital devices and the networks they connect to are at similar risks. With IT departments stretched, systems deployed without the usual security protocols in place and, a working landscape in constant flux, monitoring for potential malicious attacks is paramount.

Can businesses create digital antibodies to combat current and future cyberattacks? An answer is a multifaceted approach to their security. Remote workforces have added a high level of risk to the threat landscape but one that can be mitigated. As we wait for a vaccine to treat COVID-19, businesses need to be developing their security policies to vaccinate themselves against the next digital threat.

Read also

11 startups tackling cybersecurity in the UK

Article by DAVE HOWELL