Covid-19, Lockdown & Cybersecurity: Is The True Crisis Still Ahead?

Ongoing lockdowns throughout the world are putting digital infrastructure under an unprecedented stress. Not surprisingly, cyberthreats are on the rise but so far attacks have been managed and systems are holding. But what if the biggest challenge was a few weeks down the road when infrastructure will lack its regular updates and patches? What if the biggest threat even was at the end of the lockdown and the return to the workplace? Will our laptops and cellphones reunite seamlessly with enterprise networks and servers without massively propagating viruses and malwares? In the longer term, how will our digital infrastructure adapt to a world where digital home-/co-working will most likely be far more frequent than before?

"ALL THE WORLD'S A STAGE AND MOST OF US ARE DESPERATELY UNREHEARSED." – SEAN O'CASEY

With roughly half the planet living under lockdown, one can estimate that, approximately 45%/50% of the workforce is now staying and working from home[1]. According to large carriers[2], data traffic is spiking at 50% above average while fixed lines traffic is increasing by 30%. Within large groups and smaller businesses, computers and laptops are not only being used to access professional emails, download attachments and access visio-conference but also massively for personal purposes.

So much time spent online by so many people is an unprecedented test of resilience for our networks but also a great opportunity for cyberattackers to strike our infrastructures: +30%[3] of DDos attacks, +667%[4] phishing campaigns were witnessed in February only. However big these numbers are, all these threats are still low-level attacks, easily thwarted by current infrastructure and security procedures. And no massive breach or shutdown has yet to be reported.

But as the lockdowns extend, one can only question the ability of the system to sustain such a stress in the longer term. To enable so many people to work from home at once, CIOs and CISOs have been forced to reduce the overall level of security of their environments temporarily. To maintain an acceptable level of operations, companies have most likely had to make exceptions to hard rules: for instance authorize on-premise machines to be managed by remote system administrators. Also, maintenance and updates rely upon the execution of software patches, which are now another challenge to send and execute remotely on all the machines of an organisation. In such a context where defences are reduced and upgrades difficult to install, the highest threat is time. Indeed, the longer this situation lasts, the higher the number of vulnerabilities likely to be uncovered by cyberattackers. Other Zoom-like vulnerabilities will appear publicly only after Advanced Persistent Threat hacker groups have

[1] Google for daily commute between Feb 16th and Mar 29th; US: -38%; India: -47%; Italy -63%; France:-56%
[2] https://newsroom.bt.com/the-facts-about-our-network-and-coronavirus/ and https://www.vodafone.com/business/news-and-insights/company-news/vodafone-launches-five-point-plan-to-help-counter-the-impacts-of-the-covid-19-outbreak
[3] https://www.totaltele.com/505216/Link11-Warns-of-30-Increase-in-Length-of-DDoS-Attacks-and-Disruption-Risks-as-Organizations-Accelerate-COVID-19-Remote-Working-Plans
[4] https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

had enough time to exploit such opportunities and devise even longer term attacks going forward.

"THE FUTURE STARTS TODAY, NOT TOMORROW." POPE JOHN PAUL II

Another challenge ahead is not the lockdown per se but the end of it. Sooner than later hopefully, millions of laptops and other connected devices are going to reintegrate the enterprise networks, all at once. This is a phenomenon that CIOs/CISOs are experiencing on Mondays, after the week-ends. What will such a "Monday morning" effect look like not after a couple of days but a few weeks? For such a period of time, these devices will have been used on domestic Wifi networks (i.e. more vulnerable to attacks), sometimes hooked to other smart and connected devices such as cellphones or TVs. For the best-prepared organisations, a strong VPN will have partly insulated these devices from viruses or intrusions. A significant number of them though will contain viruses or malware, waiting to be activated to exploit yet another vulnerability to be revealed in the press weeks after.

Fast forward to a few months from now: after the sanitary crisis, an economic crisis is now in full swing. Budgets are spread thin across organisations and investment in IT systems upgrades are being pushed back. Focus is now on maintaining operational levels with lower-cost and lower-budget solutions, as opposed to the pre-Covid-19 environment where priority was increasingly on the effectiveness of the solutions above cost efficiency. In that context, upgrading or even going back to pre-crisis levels of digital security is near impossible. The shock of reintegrating millions of devices and accommodating for the longer term a more drastic shift into homeworking, the conditions for a digital perfect storm are now here.

"WE CAN ONLY SEE A SHORT DISTANCE AHEAD, BUT WE CAN SEE PLENTY THERE THAT NEEDS TO BE DONE." – ALAN TURING

From our humble outpost as a specialised investor focused on Cybersecurity and the wider Digital Trust arena, we have tried to actively listen to the intelligence gathered by our partners and portfolio companies over the last few weeks. As nodal point between investors, developers and purchasers of Cybersecurity and Digital Trust solutions, we are compelled to draw the conclusions from their observations and imagine the measures which can lower the overall cost of this crisis:

1) Take immediate measures to maintain the current levels of security within the digital infrastructure and gradually increase them back up by toughening up the conditions of security solutions such as VPN.

2) Carefully plan for the steps of reintegrating all the devices through a necessary decontamination phase, for example: plan for digital quarantines; post lockdown, keep employees homeworking so as to reduce the number of devices coming back at once?

3) Prepare for the longer term to drastically change work habits and for a wider usage of home/co-working where cybersecurity and digital safety are more deeply coded into every scenario of digital transformation within organizations, while infrastructures see their resilience capabilities upgraded.

CONCLUSION

Covid-19 and its resulting lockdowns globally took us by surprise. IT organisations need not be surprised twice. Planning now for the end of lockdown should be the priority as well as understanding the likely long term consequences of this crisis on work habits.