



STORMSHIELD

OPINION ARTICLE


CYBERSECURITY: SHOULD STAFF BE RESTRICTED FOR THEIR OWN GOOD?

Julien Paffumi

Product Management
Leader, Stormshield

Teleworking is one of the most visible signs of the digital transformations providing new opportunities within companies and responses to the health crisis we are currently experiencing. However, depending on how they are used and the way staff behave, such new applications can undermine corporate security. Should the access and functions of certain workstations be restricted to guarantee overall security? Any attempted return to the days when access and installation rights were required for a workstation may meet with some resistance. And leave IT services between a rock and a hard place.

With digital transformation, the virtualisation of services and worker mobility, the company's external borders are changing and the barriers between work and private life are now increasingly porous. Whether it's someone accessing the internal network from an unsecure Wi-Fi connection or copy-pasting a critical company document via a personal flash drive, devices are today being combined and interconnected. We should begin by pointing out that one thing is clear: this situation takes no account of hierarchy. The naive intern, the sales representative in a hurry or the CEO who believes himself infallible are all significant sources of cyber-risks. Especially as many of them have administrator rights for their workstations. We must therefore ask ourselves the following question: **should we return to "yesterday's" methods and restrict everyone for their own security?**



This question is all the more relevant in the context of the current health crisis as urgency and cybersecurity have never been good bedfellows. To enable companies to continue their activities, digital services and especially teleworking have now been shifted to employees' homes. But they haven't made the trip alone... the company's vulnerabilities are also being exported to the homes of its employees. *"With Covid-19, those companies surviving the effects of the economic crisis could find themselves devastated by cyberattacks"* warns the CISO of a major company in the aeronautical sector, earnestly. These words succinctly express the fears of the whole profession at a time when the worst health crisis for a century is sweeping the world.


"With Covid-19, those companies surviving the effects of the economic crisis could find themselves devastated by cyberattacks".


A CISO of a major company in the aeronautical sector

Let's be bold here, and point out the parallels between this unusual health crisis and the restriction of employees' IT rights. The government's decision to impose a lockdown of the population is a restrictive measure but one based on the need to guarantee collective safety and security. Could this also be a solution where cybersecurity is concerned?

AUTONOMY AND EFFICIENCY, A RESTRICTIVE ENVIRONMENT

One possible solution is making employees liable and accountable for their actions, which in certain cases may lead to disciplinary measures. But is this a desirable solution? Another option would be to return to the days when access and installation rights had to be requested for each workstation. Is this viable in the context of today's companies, in which numerous staff have direct administrator rights for their workstation? *"To understand how we got to this point in certain companies, two key challenges must be taken into account. Firstly, the wish for autonomy from some employees, who possess advanced IT skills and would like to be able to install specific applications, write scripts or prepare models without needing to contact the IT department to obtain some authorisation or other"*, explains **Franck Nielacny**, Chief Information Officer at Stormshield. *"We must also take account of a second factor, related to the availability and responsiveness of the IT teams. In some cases, an IT Manager can be extremely busy and must manage incoming requests based on priority. A simple solution to this is sometimes to grant admin rights".*






Despite this, it is recommended that a few simple rules be respected with regard to filtering and access control. *“My recommendation is a twofold one: those job categories which are not overwhelmingly technical in nature do not require administrator’ rights. For more technical users, the idea would be to have two accounts: a standard one for use on a day-to-day basis and an admin account, the latter possessing the most restrictive functions possible and strictly governed when in use by means of an IT charter”*, adds Franck Nielacny.

RESTRICT, BLOCK, HOLD ACCOUNTABLE: A THREE-STAGE CYBER SOLUTION

In a normal context, it’s difficult to envisage adopting a coercive approach involving extensive restrictions on staff. Indeed, who knows how staff would react to measures they consider overly restrictive or as violating their fundamental rights? *“Only a critical situation in which the company was in real danger could justify the use of tough restrictive measures for all staff”*, continues Franck Nielacny. *“These measures could only be temporary”*. The current context, characterised by the dual constraints of autonomy and efficiency, appears to meet these criteria for the moment: the lockdown is being accepted because the situation is exceptional and temporary.

Another example of such restrictions is the decision as to whether or not to authorise access to personal e-mail accounts in professional contexts. Once again, the midway solution would involve authorising access but prohibiting the opening of attachments, making people fully aware of the risks of infection through this channel. Because we should never forget that the risk of users trying to get round any restrictions and the resulting risks of shadow IT are never far away! *“It’s important to be realistic”*, stresses Franck Nielacny. *“We today find ourselves in a working environment in which there’s a fine line between work and private life. Shadow IT is a reality for all companies and even more so with Covid-19 and the lockdown. The challenge lies in ensuring a leakproof environment in relation to the company’s IT system by limiting the exchange of data to and from third-party systems”*. It’s therefore vital to improve awareness and responsibility from the outset. We can’t stress enough the need to instil an effective cybersecurity culture.



A GENERAL REDUCTION IN SECURITY LEVELS WITH COVID-19

In France, at a time when the hasty reorganisation of working environments to accommodate distance working is generating enormous risks for companies, on 16 March 2020 the Ministry of the Interior issued an announcement to remind everyone that an *"upsurge in cyberattacks of the "data theft" and/or ransomware variety can be expected against corporate networks, seeking to exploit any possible reduced vigilance or lack of organisation"*. *"With Covid-19, companies simply weren't ready. Most were forced to react in haste"*, added the CISO of a major company in the aeronautical sector. *"The crisis is unfolding in a context in which IT departments lack decision-making powers and in which their budgets are largely insufficient"*. With a lack of preparedness and frozen IT budgets, the health crisis could produce unexpected consequences for some businesses. Especially as in this situation, when anticipating the economic consequences the need to ensure business continuity takes precedence over IT security. As you can see, these are challenging times. In the case of strategic frontline infrastructure such as hospitals, the challenge lies in coming up with *"effective and user-friendly solutions"*, explains **Cédric Cartau**, CISO at the CHU Nantes teaching hospital, in his article on "The IT department faced with COVID" (on DSIH.fr, in French).

In addition to imposing restrictions, it's also necessary to control the likely vectors and risks of cyber-attacks. Some technical solutions make it possible to spot abnormal behaviour on a machine seeking to exploit a vulnerability, such as a sudden increase in the number of requests, user connections which are geographically impossible (such as in the late morning in Australia and the early afternoon in New York) or the use of unusual commands. It's the job of the CISO to correctly set the "standard" for non-suspect behaviour, the baseline, to bolster security without needing to restrict the user.

ZERO-TRUST, A FUTURE PARADIGM?

As we have seen, crisis situations, the changing external borders of the company and increasing staff mobility all make it necessary to rethink IT systems security. Against this backdrop, more and more people are now talking about the zero-trust approach. What does it entail? Adopting a genuine zero-trust approach to users, terminals or workstations and managing exchanges between the machine and the rest of its environment in as far as possible. *"Thanks to this model, the company can control who has access to what, how and when"*, wrote **Pierre-Yves Popihn**, technical manager at NTT Security France in Les Echos.

To conclude, in addition to protection against proven threats and abnormal behaviour, it's vital to introduce a number of restrictions on the workstations. But this must be achieved as part of an approach which also attaches great importance to raising awareness of the need for "digital hygiene" along with greater accountability for users. One of the lessons to be learned from the current health crisis is that whatever we may think, rules and personal discipline are needed to stave off a persistent threat. In a constantly-changing environment, we must also take account of the fact that the degree of "severity" of these rules can and must evolve. Adaptation is therefore the key here. To achieve this, it's vital to draw parallels with users' personal lives. *"If people firmly believe that this can have an impact on their personal life, they will be likely to repeat it in their professional life"*, stresses our colleague the CISO in the aeronautical sector.



STORMSHIELD

All around the world, companies, governmental institutions and defence organisations need to guarantee cybersecurity for their critical infrastructure, their sensitive data and their operational environments. Certified and qualified at the highest European levels, Stormshield's technological solutions meet the challenges faced by IT and OT to protect their activities. Our mission: to provide cyber-serenity for our clients so they can concentrate on their core activities, something which is vital to the satisfactory operation of our institutions, our economy and the services provided to our populations. When you choose Stormshield, you are choosing a trusted European cybersecurity provider. Further information: www.stormshield.com