Stages of cybersecurity – based on Hermann Hesse

16 April 2020 | **Cyber Security** | **Raphael Reischuk, Lena Csomor**
Reading time: 8 minutes

In these unprecedented times, when COVID-19 is running rampant around the world, the public has somewhat lost sight of the threats we face from cyberspace. But cyber attacks are more hazardous than ever before – particularly in times such as these, when remote working is on the rise. This article puts a contemporary twist on Hermann Hesse's famous poem 'Stages'.

However inescapable and characterised by fear and insecurity the news might be at the moment, there are still signs of productivity and progress. And it's digitalisation – now inevitably penetrating every nook and cranny of our (working) lives – that's providing us with the tools for precisely this purpose. It's digitalisation that's keeping educational institutions, banks and all kinds of offices up and running. People have become accustomed to their new working situations – some while simply wearing leisurewear, and others dressed up to the nines, suited and booted in front of the camera. But there's only one group of individuals that reigns supreme as the masters of adaptability: hackers and cybercriminals.

Cyber attacks pose a significant – albeit usually invisible – threat, especially during times such as these, when people are using remote desktops and working from home. And, much like the coronavirus, the threats won't stop at the front door. But being fearful is hardly an appropriate response to the current situation. There are simple ways of protecting both yourself and your employees – and with measurable effectiveness to boot. While IT specialists have often had sole responsibility for cybersecurity, the need to work from home is now forcing a growing number of inexperienced users to deal with that very issue. How beneficial and important is this development? And what technical challenges will society have to address during and after the crisis?

Bravely and without remorse to find new solutions that old software integrations cannot give

Since existing infrastructures (such as company-wide VPNs or established collaboration tools) are being overloaded, IT departments are being forced to quickly find new ways of guaranteeing the availability of services and the connectiveness of employees. This may lead to the unstructured integration of new software that the IT department and employees themselves aren't all that familiar with and for which the compatibility and security qualities haven't been adequately checked. While the solution may well appear to work on a

superficial level, the risk of dirty hacks in the system landscape still remains.

To make this situation even more complicated, many applications are currently undergoing major stress tests – which is a positive development, since software developers are being forced to build applications that are inherently more secure and stable. At the same time, this will also bring more bugs and security flaws to light, creating a longer-term benefit for application users because vulnerabilities will be patched more frequently and faster. In the short term, though, users tend to be at the mercy of more hackers, since many manufacturers are overstretched or don't have sufficient funds and resources available at short notice.

Despite all of this, IT security doesn't take the top spot in many companies' list of priorities, because – above all else – as many devices as possible have to be set up for employees as quickly as possible. Rushed processes such as these mean security flaws often fall off the radar, allowing hackers to infiltrate the system landscape. If the intruders go unnoticed, they are likely to remain on the systems even after the pandemic has passed and will exploit opportunities wherever they crop up.

Scenarios such as this one place great demands on almost all companies. But this doesn't mean they should simply resign themselves to this fact. Rather, they must be aware of what is needed in the situation. It is absolutely vital that all modifications to the system landscape are logged properly, even if no security checks are being performed at present. All new and temporarily modified devices should be treated as if they were infected with malware without anyone realising – and, accordingly, the devices should be security checked as soon as the security requirements can be met again. Systematically recording these problems allows what we might call a 'technical security debt' to be created, tracked and repaid as quickly as possible. That way, order can be rapidly restored after the initial chaos. Better still, this approach can result in a more resilient and more secure IT infrastructure that's perfectly adapted to employees' needs.

In all beginnings dwells a magic force, but it cannot guard us all on its own

Now that they've suddenly been left to fend for themselves while working from home, some people are wishing that their IT Support teams were close at hand again. Once again, employees need to be adaptable, help themselves and become more skilled in the everyday use of technology. While this process may be exhausting, it's definitely long overdue and necessary in many companies. In the long term, everyone involved will benefit from employees acquiring such new skills, as they will lead to enhanced efficiency and less hassle.

But it's important to be aware that, regardless of how tech-savvy an employee is to begin

with, everything and everyone is now being let loose on the unfiltered internet – and this is a source of major risks, because employees are now mostly learning via work equipment. So it's in employers' interests to provide their staff with a certain amount of basic knowledge (not least in the field of IT security) in a comprehensible and simple manner and as quickly as possible. The ability to assess and identify risks should take top priority in this respect. Companies are also facing new challenges due to the work equipment itself. After all, when is work equipment defined as such? In the simplest (and most secure) case, employees have taken their usual device home from the office, so it'll have the same security standards (at least locally) that were previously established by the company. 'Non-local' work equipment is particularly at risk, especially when staff are working from home – when the boundaries between their private lives and professional lives often become blurred. It must be assumed that users will be less disciplined, download unsafe software or click on dangerous links against their better judgement. After all, when people are at home, they're in familiar surroundings and therefore feel safe – even from cyber attacks.

Things take an even more dangerous turn when private devices that aren't well secured suddenly have to be used for work purposes. In such cases, business data is being loaded onto untrusted devices, where it might even remain for a long time after the pandemic has passed if the user forgets to delete it. This is why it's important to point out (when employees return to the office at the latest) that staff should also 'tidy up' their private devices.

The list of problems is long, and handling sensitive data is high on the agenda for some companies; they've had to go paper-free in some of their processes within an extremely short space of time. Documents and other data are now being sent entirely by email; fax machines have finally become outdated. It's safe to assume that many employees received insufficient information about processing sensitive data by email, because this data was previously only available on paper and in protected databases. The fact that everyone is now working in their own network (which isn't being monitored by their employer) means that cybercriminals have a much larger target than they did before the coronavirus pandemic started. All it takes is for one home network to be infected and hackers will have a field day, accessing valuable data and confidential communications. If this data is stolen now, this can have long-term consequences for the companies and, accordingly, for their customers. Virtual desktops are one possible solution when private devices are being used for work purposes. While this doesn't solve the problem of employees lacking awareness, it can create an environment that's more secure in technical terms and gives some control back to the company.

And life may summon us to newer races

Since they don't have other activities to keep them occupied and their parents have laptops, more children are learning long overdue IT skills such as programming. Parents are posting

numerous photos of their children wanting to be like ‘the grown-ups’ and sitting next to them at the computer. Many (especially those who are tech-savvy) are then even encouraging their children to find out more about the device and its functions. Homeschooling is promoting the need for children to be able to use computers and tablets independently. And that they do, often at alarming speeds!

Security problems will always exist. Today’s children are definitely prepared for working from home – as long as we, the grown-ups, set a good example. There’s a wealth of possibilities that goes hand in hand with being forced to work from home. It’s extremely important that security takes top priority and isn’t repeatedly pushed aside due to time constraints. Let’s take the necessary time and make the world a safer and (hopefully) healthier place.

Headings freely adapted from the wonderful poem ‘Stages’ by Hermann Hesse, which gives us courage in every crisis.