GREYCORTEX CTO
On securing the home-business network

The emergency provisions related to COVID-19 have been active for some time and more and more companies are allowing their employees to work from home. We asked Our Chief Technology Officer Vladimír Sedláček, a seasoned administrator of ICT, corporate systems, cybersecurity, and experienced developer, about his opinion on current affairs.

The Coronavirus pandemic impact is discussed everywhere, but few people seem to realize that despite all the physical risks, digital issues still present a significant problem. How do you see the current situation, and what do you consider to be the biggest risk in terms of virtual infections, and their possible outcome for companies?

It would be naïve to assume that the global crisis would lead to a drop in cyberattacks or will result in a ceasefire. On the contrary. In nature, each weakened individual becomes prey. Regardless of any previous "ceasefire declarations", we see an increase in the number of attacks and targeted at the SARS-NCov-2 situation.

Obviously, we can expect contacts from faux health inspectors and money collectors. Even my inbox has received several phishing emails offering nano-silver infused masks. In addition to attacking the weakest part of cybersecurity – the user – we also see an increase in scanning; looking for vulnerable computers and security holes in firewalls or hastily constructed VPNs and remote desktop gateways.

In the end, all of this contributes to latent disclosure of company secrets, production and patent documentation, or personal data. Infiltration by extortion malware also becomes a threat and can mean a total production halt, as seen both last year and recently in some hospitals in Czech Republic.

What do you see as the most common errors from employers and top management regarding data exposure; and how does the risk increase with massive deployments of quarantine provisions where most employees work from home?

Right now, the risk is increased by companies laying off contractors, often those working on infrastructure, promoting rotating furloughs, and allowing their administrators to work from home. This can cause a delay in necessary security patching and increased response time. Also, ad hoc suspension of certain user accounts can leave the access ripe for unauthorised access restores later.

Last, but not least, some companies have allowed their employees to work from home using their home computers. VPN has thus become a gateway for free access directly into company networks, and to internal company systems, all thanks to home devices with uncertain security postures, possibly outdated operating systems, obsolete software, or a load of games full of spyware. These systems are being used by home-bound users surfing the web with local superuser rights.

It is very similar to allowing the usage of personal devices (BYOD) and letting them directly connect into internal, as opposed to guest networks. A lot of companies do not, however, tackle the situation accordingly, and have not familiarized their employees with relevant security policies.

Without in-depth employee training and without respecting the basic rules of cyber hygiene, internal data can leave the control of responsible people working with it.

What has not received much attention so far is the risk of company device theft in conjunction with wiping such devices clean. Partly due to the fact that the employees "stay home" and are convinced that they have good visibility over their physical environment. However, thefts will happen, and the security angle will need to be tackled.

I cannot understand why so few administrators allow internal networks to stay open, and who pay attention to their internal network traffic with only commonly used tools for network monitoring. Same tools that are deployed normally are themselves a potential attack target.

In your professional career, you have seen quite a few approaches to computer networks and have seen quite a lot of disasters. Can you share some practical examples of some really serious company infrastructure breaches and what disaster recovery measures took place to ensure network security?

In the small business segment, the common practice used to be that on the LAN perimeter there was a small, general purpose machine with a public IP acting as several components, including a firewall. When a router costs the same as a used car, it is just about the only affordable solution.

Let me give you an example: The machine in this instance was Linux-based, with public-facing SSH allowing for remote administration as well as acting as a mail server for sending and receiving emails for mailboxes. In addition to the operating system and applications being out of date, the server contained a list of all users with operating system-level access. All mail users were also included. Back in the day, postal clients sent their credentials as plain text in unsecured channels. All you needed was to eavesdrop on this transmission once, and there went your password for mail as well as the operating system.

After logging in using SSH, anybody would immediately gain access to the mailbox, and through it to the internal network.

In compliance with the latest recommendation of separation of duties and segmentation, I installed a separate firewall – back then, a thousand Czech koruna expense – and moved the entire electronic mail into a demilitarized zone. I also deployed an encrypted mail transfer. In the virtual user account management system, I further separated accounts for sending and accessing emails from accounts for operating system access. The entire project was thus done quite cheaply and in three days, including two days of migrating individual users' messages and configuration changes. Shortly after switching the old server off, some competitors "miraculously" lost their ability to beat our offers.

What would you recommend to top management and employers regarding data protection in the home office era, and what do you see as the most critical and vulnerable points nowadays, when a lot of companies have suddenly switched to remote working? Is there a simple solution, or do you need to combine tooling?

Honestly, in security there never is a silver bullet solution. It always depends on the current situation, how the company handles its data, and finally on its infrastructure. Someone who has managed to segment their internal network and solved limitations on accessing sensitive systems within internal network segments has a much better pole position than someone who keeps all devices and functions on a single network. Of course, in addition to technical security, you need to maintain employee awareness. That can be done quickly, similarly to how you can rent "bare" computers from technology vendors. Companies that suddenly allow employees to use their own private devices for working data that needs to be kept inside an internal network, need proper measures. In addition to last minute VPN deployment, they should consider "clientless" access system to remote desktops using web-based interfaces, like guacamole.apache.org, which is free and can be configured for safe data transfer.

No matter what work from home solution, VPN and remote accounts should be different from common working accounts, or at least require different passwords. Beyond limiting access to internal resources access from VPNs based on the signed-in individual, I would also strongly recommend deploying a sophisticated network monitoring and discovery tool.

Based on your observations about the world situation, what direction do you expect remote work, education, and business to take, and what potential hazards will we have to prepare for?

I suppose that for some companies, the process of informatisation and internetization will speed up. Whenever remote work is possible and will prove efficient, it will probably prevail. It might be prone to limitations, but I am optimistic.

Perhaps we will get to the point of acknowledging that instead of four hours spent traveling to an hour worth of meetings and back, we can better utilize conference rooms equipped with expensive and high-end teleconferencing equipment, and that such rooms will eventually become available to the general public for a price comparable to traveling in person to the meeting.

Cloud-based services promoting online collaboration will show their strengths. New platforms will flourish based on these; orienting themselves on connecting supply and demand on a minuscule, locally dependent scale. However, even the cloud platforms of today face their limits; namely in finite computational and transmission capacity. In the long term, we might expect a shift from large, remote data centres to structures closer to the end user.

What about cyberthreats? Phishing campaigns will change their contents; the executed malware code will intensify its search for VPN or remote desktop credentials. It will emphasise targeting collaborative platforms and cloud services. But the basic foundations of today's cybersecurity will likely remain unscathed:

- Each device has its own perimeter that it must defend on its own
- Protection of my perimeter protects other network participants
- Organisational networks, no matter how small, must be segmented with regards to data sensitivity
- Trust nothing and no one, especially not simple passwords
- Services cannot be federated on a whim and access to them is to be restricted and monitored
- Every transmission must be encrypted, and the participants need to be verified
- Attack preparation and disaster recovery awareness is a must
- Back-ups are necessary, but useless without deployability checks
- Users must be kept educated
- Users' and device activity must be logged independently on each other
- Network behaviour has to monitored and analysed with a system external to the operations traffic layer

GREYCORTEX

Ing. Vladimír Sedláček is an experienced developer, analyst, and administrator who has worked to connect diverse systems and develop a secure web platform and infrastructure for more than 100 million clients. His passion for cyber security and hacking has led him, among other things, to passing the Certified Ethical Hacker and Certified Livewire Investigator exams.