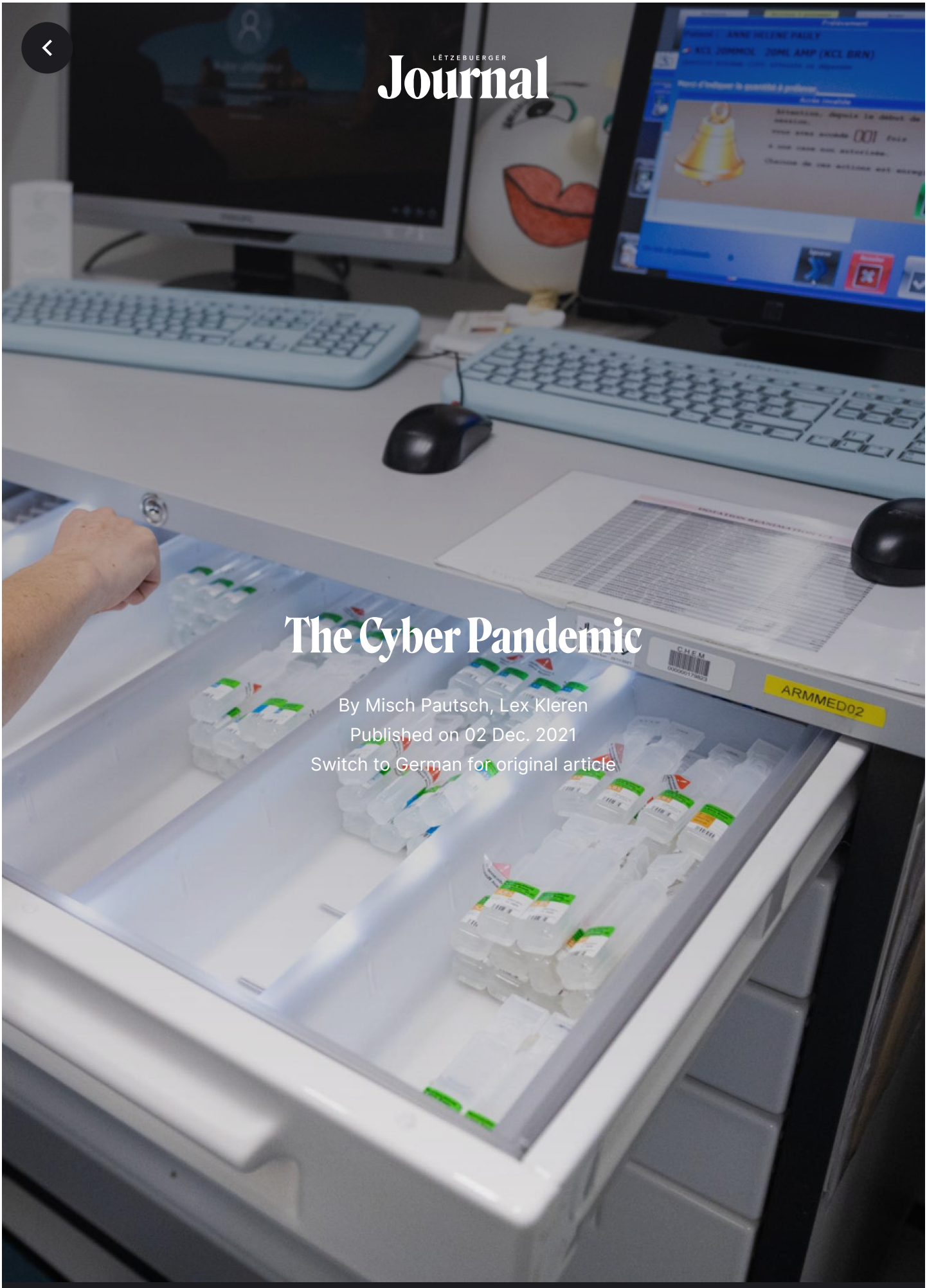
LËTZEBUERGER Journal



The Cyber Pandemic

By Misch Pautsch, Lex Kleren

Published on 02 Dec. 2021

Switch to German for original article

Listen to this article

09:49

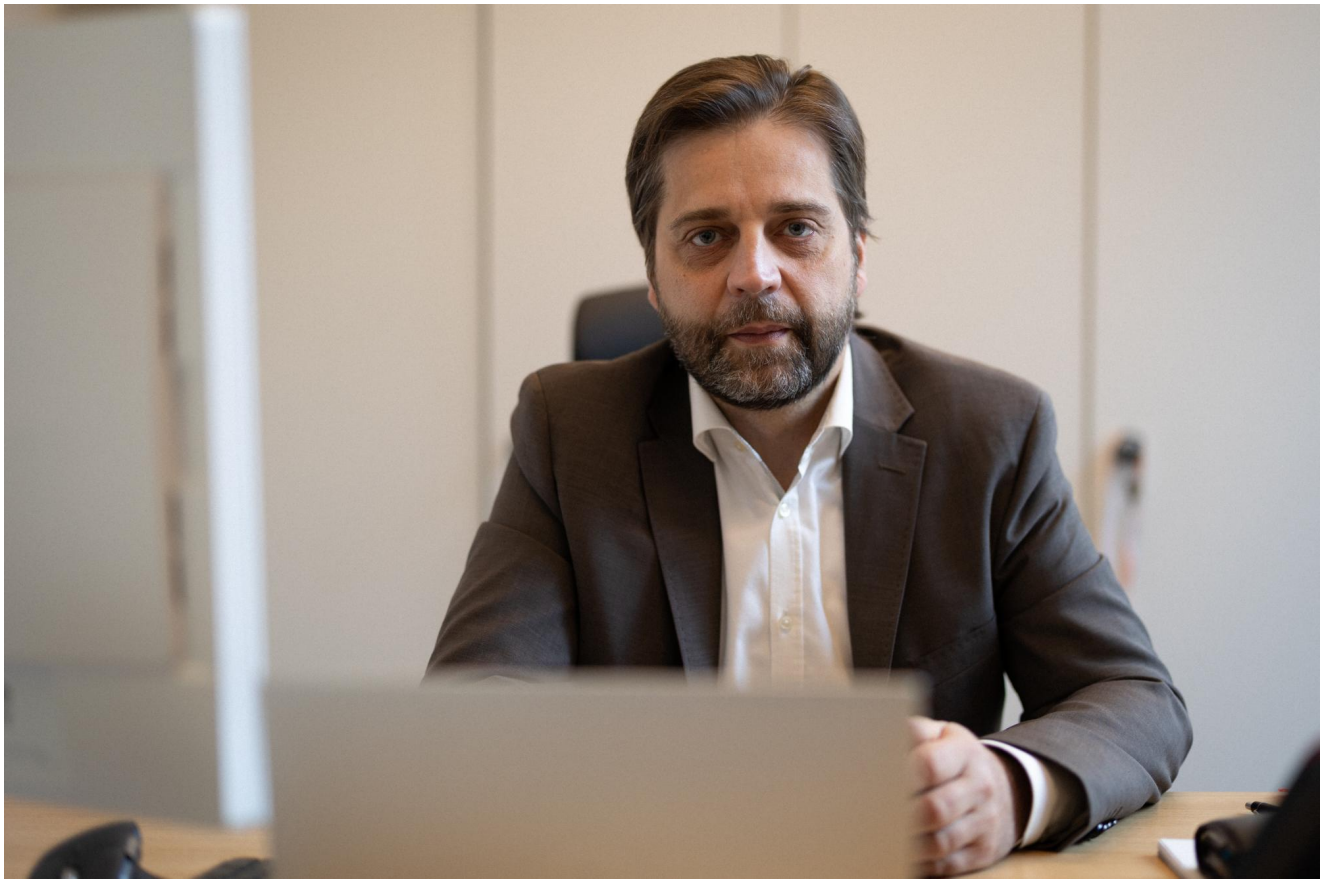
The number of IT attacks against hospitals worldwide has risen dramatically over the past two years - in some cases with deadly consequences. Luxembourg's hospitals have been able to successfully fend off attacks. But the fight against the organized, often state-supported gangs goes on. The pressure is rising.

Behind the scenes of the already dramatic scenes in hospitals, a second, invisible battle is being fought daily: Organized cracker groups are capitalizing on the pandemic to ramp up their attacks against healthcare. Before the pandemic, ransomware attacks, which lock users out of their infected computers until they pay the crackers a ransom – infected computers display a "handy" help screen listing steps to unlock them – were programmed to aimlessly hit as many people as possible: The more victims, the more ransom. Now the focus seems to have shifted, says Paul Rhein, the director of the Governmental Computer Emergency Response Team (GOVCERT), which reports to the Office of the High Commissioner for National Security: "The big change over the last few years is that the focus has shifted from private citizens to businesses and organizations."

Large-scale ransomware attacks are not limited to the healthcare sector, as evidenced by the attacks on the largest gasoline pipeline in the U.S., the Colonial Pipeline, or meat processing plants owned by JBS, the largest meat processing company in the world. In these "campaigns", coordinated computers in the U.S., Canada and Australia were blocked, both times with devastating consequences for far-reaching supply chains. "Especially now, hospitals are an attractive target for cyberattacks", Rhein explains. In heavily burdened hospitals, even small failures can lead to serious human harm: All the greater is the incentive to pay the ransom – after all, human lives are at stake.

When computer viruses are deadly

At least one case in Düsseldorf shows that these fears are not unfounded. Here, a woman had to be transferred to another hospital after a ransomware program took down 30 of the hospital's servers. The delay ended fatally for the woman. While further investigations revealed, that the woman would have likely died regardless of the attack, the case nonetheless reveals how shutdowns can cripple caretakers. While some groups had announced a "Corona-break" at the beginning of the pandemic, it now seems to have turned into the opposite. "These attacks have high costs on all fronts", writes the Geneva-based CyberPeace Institute: "resources dedicated to fighting COVID-19 are crippled, patients' safety is impacted, sensitive data is stolen, and overall, society loses trust in its healthcare system."



Paul Rhein, GOVCERT.lu

"Unfortunately", Rhein laments, "the perpetrators behind such attacks are rarely brought to justice." For the crackers, such attacks involve low risk and very high potential reward: Ransom demands can reach into the millions, and cross-border investigations beyond EU-borders are extremely difficult.

The number of cyberattacks against hospitals has increased significantly since the start of the Corona pandemic. Between November 2020 and February 2021 alone, the number of attacks against the healthcare sector through various cyberattacks such as "ransomware, botnets, remote code execution, and DDoS attacks" that damage networks, systems, or computers in various ways, increased by 145 percent in Central Europe, according to Check Point. German hospitals were hit by 220 percent more attacks. Coordinated attacks in the United States have forced some doctors to resort to handwritten notes for days, operations became impossible, organisation and coordination broke down for hours or days. Such attacks have also become more frequent in Luxembourg, Rhein confirms. "Very currently, an attack campaign called 'SquirrelWaffle' is ongoing, which among other things installs 'dropers' or 'trojans' on affected machines."

This situation could develop into a major ransomware campaign, he adds, because ransomware attacks are only the final stage of coordinated attacks: cyberattacks usually consist of several repetitive stages that can be more or less sophisticated: Spying, infection, stealing files, and/or encryption, extortion, and defacement (an attack on a website that changes its appearance, comparable to "electronic graffiti", editor's note). These happen in waves, in principle, and are particularly pronounced when "new or particularly performant software has been developed or adapted, such as the software called 'Emotet.' In principle, such attacks are not limited to just one sector", says Rhein.

> **"A work network could be infected by a work laptop that was hooked up to the same network as a private, infected laptop only a single time."**
>
> Dennis Fink, Chaos Computer Club Luxembourg

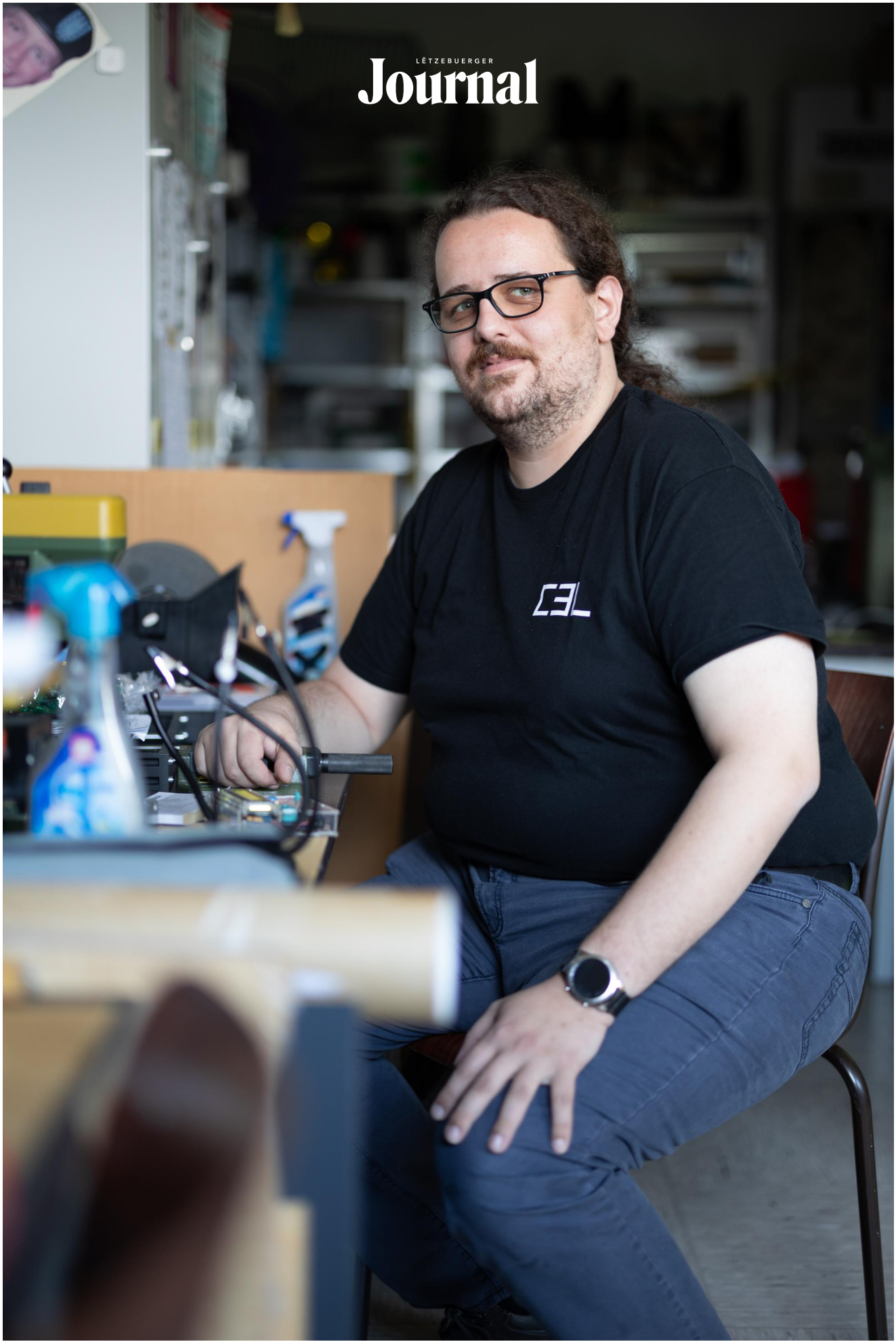
Dennis Fink of the Chaos Computer Club Luxembourg (C3L) describes how perfidious malicious programs can be: "With performant malware, we see that it does much more than just invade a single computer. A case at a hospital in the UK in 2017 showed how software automatically scanned the network for further vulnerabilities from an infected device. For example, a work network could be infected by a work laptop that was hooked up to the same network as a private, infected laptop only a single time." Once

the almost invisible program has spread across the network, it paves the way for other software, including ransomware, to be activated in all infected machines at the same time – without the owner of the first infected machine ever knowing that their computer was patient zero.

In addition, Fink explains, hospitals generally tend not to update their software immediately – one of the most important preventive steps against infection: "I don't know exactly what the situation is in Luxembourg, but hospitals tend to work with older software versions because they prefer systems that they are sure will run reliably." Updates could come with compatibility issues, unknown bugs (system errors) could creep into critical machines "and it's not so convenient if the technician has to update all the machines by hand every few days. So they'd rather work with old, reliable versions that work reliably. There's nothing inherently wrong with that, as long as the system is well isolated from the Internet … which I strongly suspect is the case for hospitals."

Fullstop

In a worst-case scenario where the entire operation is stopped from one moment to the next, Fink says, generally "depending on the type of software, there's not much you can do except fall back on backups – if they weren't also locked down at the time of the attack – … or pay. Surprisingly, it seems that in most cases people actually get the password sent to them as soon as they wire the money." The crackers pose as warped "service providers" who "give" people their data back and, accordingly, want their "customers" to be happy. Often, the unclickable window listing the steps to unlock the computer – after the virus has become active – explains that the computer was locked "to protect the files" because it had been infected by another malicious program. In return for this "protection", one should now pay the specified sum to the unknown benefactors who "protected" the computer. Obscene irony.



Dennis Fink, Chaos Computer Club Luxembourg

However, according to GOVCERT Director Paul Rhein, the real motive behind cyberattacks is almost always money: "The extortion attempts are mostly about financial interests. Of course, it cannot be ruled out that other aspects may play a role, as we have seen in some situations abroad. At present, however, we always observe in our country that the ultimate aim is to extort money. We are now confronted with a real ecosystem where different actors offer different illegal services to enable other criminals to ply their trade."

According to experts, there seems to be a safe haven for these criminal organizations: Russia. Because many "ransomware gangs operate from Ukraine and Russia", according to cybersecurity experts – with the Kremlin's silent approval in the eyes of many analysts – Russia was excluded from a meeting of representatives from 30 countries on cybersecurity and defence against ransomware in October 2021.

An unusual way to protect against such attacks underpins such accusations, speculates Dennis Fink of C3L: "If you look at the code of many of these viruses, you find that there is one very precise criterion that prevents many of them from becoming active: Russian keyboards. In fact, that's one of the main criteria that many viruses looked for. So they seemed to very specifically exclude Russian-speaking computers from their campaigns. Presumably because that would get the gangs in more trouble with the state than it's worth to them. Speaking of which, I still have to get one of those."

"The extortion attempts are mostly about financial interests. We are now confronted with a real ecosystem where different actors offer different illegal services to enable other criminals to ply their trade."

Paul Rhein, Director of GOVCERT.lu

For critical infrastructures like hospitals, however, installing Russian keyboards is obviously not a winning strategy. The task of keeping an eye on such important

systems falls to GOVCERT, as its director explains: "Our goal is to provide the best possible protection against cyberattacks for all organizations that fall within our district, while being fully aware that 100 percent security cannot exist. What man creates, man can destroy. But the last and only Ransomware infection from one of our customers' laptops dates to 2017. In that case, isolating the machine and reverting to backups did the trick." In general, he says, backups and isolation of infected machines are the main mechanisms when prevention and detection have not been enough.

Contingengcy plan

"In the event of a coordinated attack on the entire healthcare sector with a significant impact at national level, the High Commission for National Security has drawn up the 'Plan d'intervention d'urgence Cyber (PIU Cyber)' to deal with this situation as well", explains Paul Rhein. So far, however, this has not been necessary: "To date, none of the numerous attackers has managed to encrypt data under our supervision or obtain a ransom."

In the final instance, however, Rhein stresses that the "legal responsibility lies with the 'owner' of the IT system". And those prefer to play it close to the chest: When asked by the *Journal*, the Centre Hospitalier Emile Mayrisch (CHEM) only confirmed that their IT teams were aware of the risks and that they were monitoring the situation together with GOVCERT (the central contact point for all types of IT incidents that could endanger the information systems of the government and other public or private infrastructure operators classified as critical). The other hospitals did not want to comment on the issue at all.

"Cybersecurity is a process", summarizes the GOVCERT director, "never an achievement." Increasingly frequent and sophisticated attacks will certainly not make this process any easier in the future, especially when hospitals are already stretched to their limit.

Published on 02.12.2021
Updated on 15 Dec. 2021 at 20:33

Misch Pautsch

Journalist and photojournalist

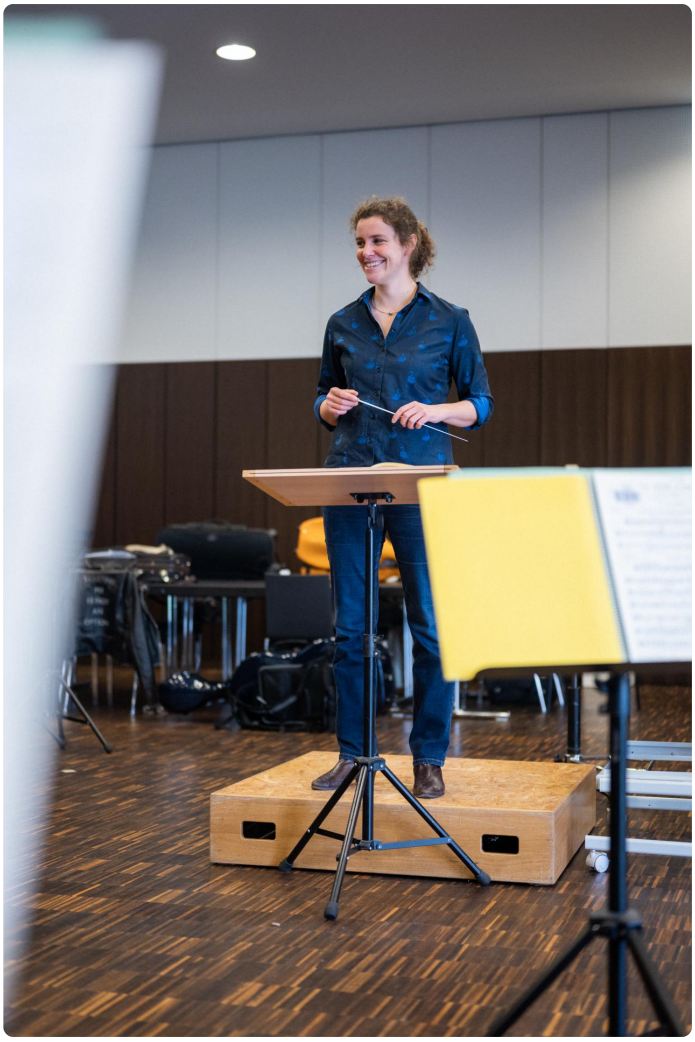
Lex Kleren

Photojournalist and editor

safety health society cybersecurity ransomware cert govcert paul rhein chaos computer club dennis fink luxembourg misch pautsch lex kleren

RELATED ARTICLES

Explore



READ

About beats and batons

By Audrey Somnard, Lex Kleren
Published on 30 Apr. 2021