When real time means: In a second, you will be dead

Thomas Tschersich, Head of IT security at Deutsche Telekom, on imminent attack scenarios in the near future, failures of the past, and “basic homework” of the present.

Photo: iStockphoto

COPY —— Thomas Tschersich

To get straight to the point, there are only two kinds of companies today: those that know they have been hacked and those who do not yet know. Period. This is because the increasing complexity of our systems makes it very easy for hackers. Especially when the vast majority of victims have not even done their most basic homework. This is why around 95 percent of all successful attacks today are based on the fact that software updates are not downloaded or are downloaded too late, or that a system is poorly configured. So much for an overview of Germany’s corporate landscape. And it is not only about the operating system, but in companies sometimes about several hundred programs, which must be kept up-to-date and maintained. Where, just a few years ago, we had months after discovering a weakness to download an update, today we have a few hours. It no longer takes a hacker any longer than this to reverse engineer what weakness in particular is closed by an update and to program an appropriate hacking tool. And if things continue to develop this way, we will experience fully automated attacks from the moment of release in the next five years. At the latest by then, we will say, “Welcome to real time! In a second, you will be dead.”

In other words: As quickly as we plan for real time scenarios coming from a threat, we also need to be able to react as quickly. Businesses no longer have an excuse: Statistics show that more software failures occur because NO updates have been downloaded than the reverse. Moreover, simple yet clever strategies in rolling out updates have long since offered drastically reduced testing periods to win the much quoted race between the tortoise and the hare – and all of it in real time.

REAL TIME MEANS AUTOMATION

This development makes one thing clear: I need to continually adapt the shield I have placed over my company. Objective security is always only a snapshot and is never sustainable as the status quo. Security is much more about the lengths to which I go to protect my employees and their devices, my processes, data, company secrets, and customers – a perpetual motion machine. And there is always a time pressure under which we need to keep it in motion. It begins when an attack is detected. This is why, in a security context, we invest a lot of money into automation. Real time means nothing but automation – to have my sensors automatically detect attacks the moment they begin and, ideally, automatically implement countermeasures. In this context, real time means I need analytics that evaluate sensor data in real time and are capable of reacting in a way that helps me use analytics to convert the sensor data into a response. Immediately. One very good example of this, because it is extremely challenging for us, is what are called APTs, or advanced persistent threats. These are new, unknown attack patterns that want to infect me with malicious software, for example, through a weakness in my PDF reader that has not been patched. I can detect this by virtually opening a document on a computer during transport and running a behavior-based analysis. If it behaves in such a way that it obviously wants to make changes to the operating system, then it is probably malicious, and I would block it. In this case, I would have already analyzed the harmful effect in real time, but the trade-off is a poor user experience. This is because taking a document or whatever a user downloads from the Internet out of circulation takes just a few seconds. However, this is a price we do not usually want to have to pay, which is why today we let the documents get to the recipient and analyze them at the same time. Consequently, I am no longer working in real time and may only determine a harmful function seconds later. But now I have its pattern and can block all others that follow in real time. In other words, I lose the time needed to analyze the first one, but I can detect the second, third, fourth, and fifth on the fly in real time: These I just block, they do not get through. Then it is just a matter of dealing with the first one, the one that got through, which I need to repair later or put under quarantine. This is an example of a strategy of how analysis only works in near-real time for the first one but does work in real time for the second, third, fourth, and fifth times.

PREDICTIVE PROFILING: THE HIGH ART OF CYBER DEFENSE

Today, machine learning algorithms help us a great deal with creating predictive profiling. That is, using traffic data, traffic volume, and behavioral information to predict what is likely to occur soon if hackers had it their way. Then I would actually get a bit closer to the real time window to block the attack before it has actually occurred. Being preventively prepared in this way and possibly being able to say, “Something is brewing here” ahead of time, is the job of a monitoring center. Its task is to provide managed cyber defense services: proactively tapping data sources, correlating them with one another, and using the result to be able to predict attacks – in real time if possible.

One technologically simple yet massive problem by comparison are devices that I call “fire-and-forget” devices. They turn our private home environment into a parade ground for cyber attackers. Practically no one addresses the topic of security when talking about networked baby monitors, for example. No one is interested. Updates? Nope! They are in hundreds of people’s homes and are easy for attackers to hack in order to carry out attacks against others. And when hundreds of baby monitors send requests to your website, it can be overloaded in the blink of an eye and your company's website is now down for hours.

For me, this is the dark side of unfettered digitization. Or you could also say digitization without rhyme or reason. This is what leads to refrigerators sending spam or baby monitors carrying out attacks against infrastructure. To say I am going to stop digitizing because the attack surface is too large is no solution. Digitization done intelligently means I first look at the risks and consider how I can network something – when it makes sense to do so – in an intelligent way. Basically going on a digital interface diet.

> **"Digitalization made intelligent means I'm dealing with the risks first and thinking about how I can network what intelligently."**
>
> **THOMAS TSCHERSICH,**
> Head of Group Security Deutsche Telekom

By answering questions like "Where do I maybe need to install a shield?", "Where do I just need to sever communications or reduce them to a minimum?" And sooner or later, I will need to pose the fundamental question: Do shutters, home solar panels, and coffee makers need to be accessible to anyone in the world? In most cases, there is no sensible application scenario for this. Ultimately, only I, the user, should be able to access my home network to look at the components and see how much power I produced today. In this sense, a smart design would preclude my refrigerator being accessible to unauthorized outside parties in the first place and the additional attack surface to the outside would therefore be prevented. So far, this has been missed on a number of occasions. For more digitization need not mean new exposed flanks – as long as you invest a little care.

SURRENDER IS NEVER AN OPTION

Investment is a good keyword here, especially considering there is enough capital and technological know-how in Germany to effectively shut down the risks of cyberattacks. However, both also need to be invested. In the end, knowledge only hurts the one who does not have enough of it. And this illustrates that those who do not obtain this knowledge become victims more quickly. Translated into cold, hard cash or technology that also make sense to be used in a company, there is no magic formula for the solution. The solution depends on the company's specific needs, the level of automation, the business models, etc. But if my annual security investments are not somewhere between two and seven percent of my IT expenditures, then the alarm bells in my head should be going off as an entrepreneur, because I would then be dropping below the standard that is generally seen as healthy.

Resigning to some putative superiority of cybercriminals would definitely be wrong. No one should be put off by the fact that 100 percent protection is impossible. Let us stick to what has led countless startups – including ones in the area of security – to success: Practically anything is only impossible until someone comes along who does not know it is impossible and simply does it. There is much truth to that.

To put it another way: When it comes to cybersecurity, whoever fails to draw the right conclusions in just one single area can very quickly have all the time in the world, since, from a security perspective, they have likely underestimated the factor of real time and will then have some "real time" to fume about it.

Thomas.Tschersich@t-systems.com

Vita

Thomas Tschersich, who has a degree in electrical engineering, has been Head of Internal Security & Cyber Defense at Telekom Security since 2017. He previously held the position of Chief Security Officer of the Deutsche Telekom Group. He is a member of the Cyber Security Council, the UP-KRITIS Council and Chairman of the Security Steering Committee at BITKOM.

Photos: Deutsche Telekom, POLYGONVATRO GmbH