



Azkoyen Time & Security Division



**Time to take the security
of your company seriously**

Don't leave your access control out in the cold

***"We take care of you,
while you take care
of your business!"***



Time to take the security of your company seriously

Cyber security, the subject that tech journalists, experts and almost everyone who is involved in ICT in one way or another, can't seem to stop talking about. After some unfortunate incidents, data leaks and other breaches over the past few decades, keeping digital infrastructure secure has become a top priority for almost every company. And because the world of cybersecurity is erratic and changes strongly from year to year, most (large) companies do not hesitate to invest lots and lots of money in digital security measures. It is an understandable way of thinking, which all too often results in physical company security, such as access control, lagging behind. Because, "Employees have their own badge that they use to enter. And that has been going well for years, in the same way. Why change now?". This is a common statement when the topic comes up. And there is, unfortunately, a dangerous mistake in this way of thinking. A mistake that can lead to irreparable damage and a lot of unnecessary suffering... ■



Access badges can also be hacked

"If it works, it works". That is the approach with which many companies approach their access control. Employees receive their own badge that opens the doors, so that unwanted visitors are left out in the cold. And that has been going well for ten, fifteen or even twenty years. And so, at first glance, there doesn't seem to be any reason to do things differently. The world of cybersecurity may be changing rapidly, but the old, trusted badges and readers just do their job. Don't they?

We see this way of thinking a lot. And that probably has to do with the fact that many companies (and even the ICT experts there) may not be aware that access badges can also be hacked. Because not only cybersecurity is constantly changing, criminals are also increasingly using digital means to gain access to physical locations. And that can now be done "just" with the smartphone. An example: as a cybercriminal, with the right application, you only have to hold your mobile phone against the pocket of an unsuspecting employee to copy all the data that is located on the outdated access badge in that pocket. After that, this criminal can copy the access badge one to one.

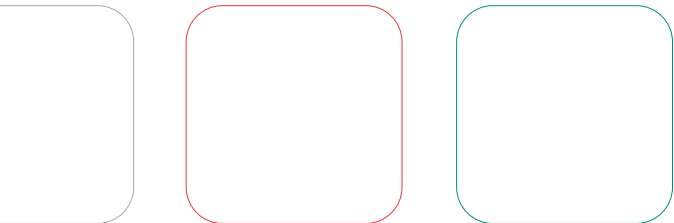
And all this, without the unfortunate employee whose badge has just been copied noticing. It seems unlikely, but this is just one of the risks you run if your access control system is older than fifteen years, or even ten years. ■

Because not only cybersecurity is constantly changing, criminals are also increasingly using digital means to gain access to physical locations.



Millions to cybersecurity and yet a break-in

Old badges can be copied with the greatest of ease. And that has disastrous consequences for the safety of your company. After all, an old badge reader will never recognize that a badge has been copied. And that ensures that criminals can quite literally just walk in through the back door, or even through the front door. And all doors in your building will open as normal, just as they would for the employee whose badge has been copied. And once a criminal is inside, things can move fast. Hypothetically, a USB stick with malicious software is now all it takes to shut down your entire business, or to steal valuable data or even money. Once the criminal is inside and the doors are open, all that person needs to do is find a PC connected to the local network. The USB can then be inserted into the USB port and the damage is done. Not even the best cybersecurity can do anything against such an intrusion. ■



False accusations and emotional damage

Your access system's data log can probably track which doors have been opened at a certain time. And once the intrusion has been discovered, it makes sense to look at the responsible badge. And you will see: the traces then all point to your unsuspecting employee, whose badge has been copied. Subsequently, he or she is wrongly identified as a suspect and, in addition to the material damage, the emotional damage is also severe. For example, if the employee in question does not have a verifiable alibi, this may result in a lengthy and drawn-out investigation. In short, as a director or head of the ICT department, you want to avoid this situation at all costs. And then all arrows point towards improving your company security. ■



New technology is virtually impenetrable

For the safety of your company, it is unthinkable that you invest millions of euros in cybersecurity, only to ignore the fact that your access control is totally outdated. That can and must therefore be done differently, for you, your data and your employees. That is why it is time to you have your badges, badge readers and the underlying infrastructure replaced by newer, safer techniques such as the MIFARE DESFire. Your employees can simply open the doors with their own badge or access pass, just like before. However, these new techniques cannot be hacked or copied, because they are encrypted with state-of-the-art encryptions that, just like your old software, will last for years. And thanks to technological innovation, new badges also offer new advantages, such as uploading a balance for payment in the canteen. This not only makes your company safer, but also friendlier to your employees. ■

***For the safety of your company,
it is unthinkable that you invest millions
of euros in cybersecurity, only to ignore
the fact that your access control is
as leaky as a basket.***

It's time to really secure your business

Let's start by saying that it is of course very important that your cyber security is in order. However, once your company's access control is very outdated, the many layers of cybersecurity can unfortunately do nothing. And then your company still runs an unnecessary risk of burglaries, with all the consequences that entail. Fortunately, there are newer, safer techniques that really keep your company safe, without structurally changing the way your employees open the doors in the morning. But one thing is certain: criminals will really be left out in the cold this time. ■



Are you ready to really secure your company?

Then we would be happy to talk to you to discuss the possibilities.

This will make your company impenetrable on all fronts! ■



Continue to talk together?

Then you can call us on **+32 (0)3 312 92 30**.

We look forward to speaking to you!



Azkoyen Time & Security Division

GET nv

Antwerpsesteenweg 107

2390 Malle, België

+32 3 312 92 30

info@get.be

www.get.be

GET Nederland bv

Albert Einsteinweg 4

8218 NH Lelystad, Nederland

+31 320 25 37 90

info@get.nl

www.get.nl