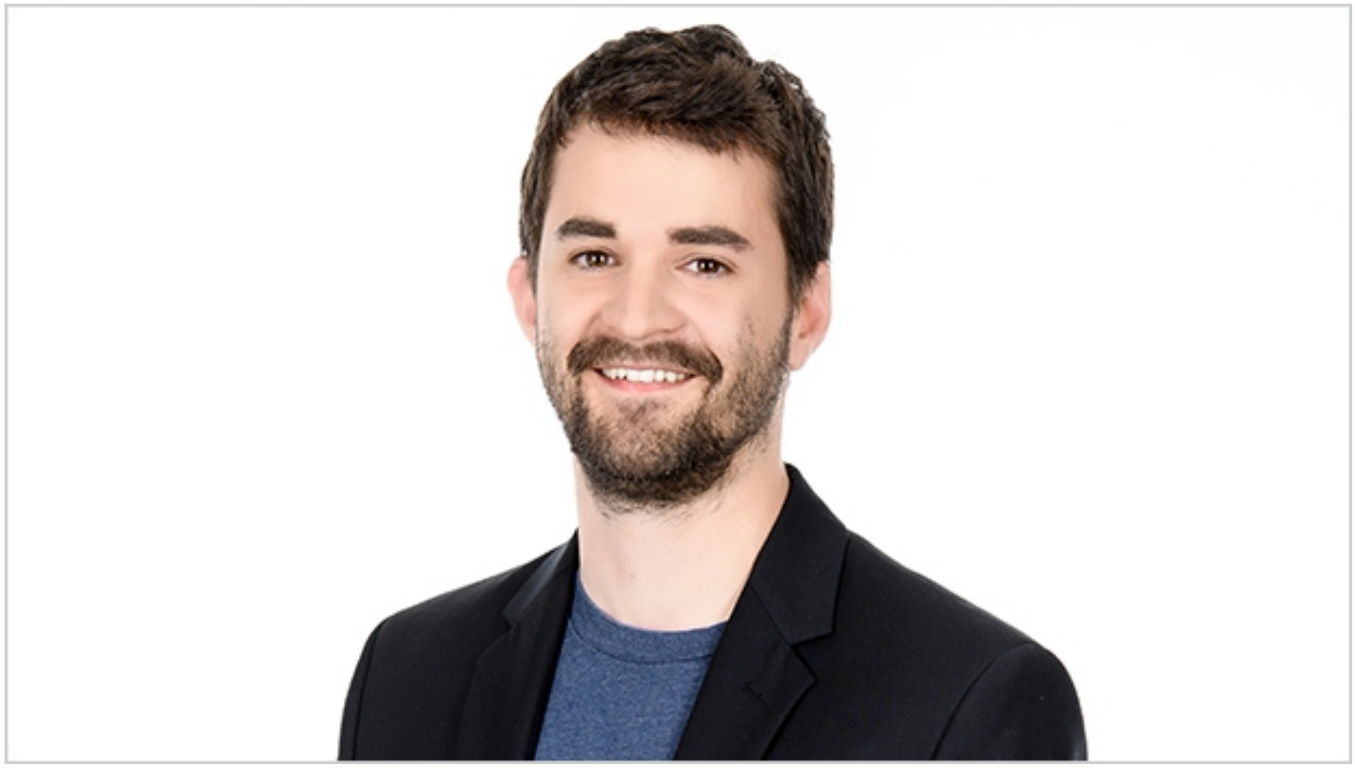
Interview with European hacker: “Investing in cyber-security is like an insurance”

As things get more digital and everything is connected, the potential for cyber-attacks grows. We speak to Aron Molnar, Security Expert at A1 Digital and leading European hacker, on what retailers should be on the lookout for.



Aron Molnar studied IT Security at the University of Applied Sciences, where he took part in various hacking competitions. With his Austrian team they won the European Cyber Security Challenge a few years ago. When he finished his studies he joined A1 Telekom. For three years he has now been working on security at A1 Digital.

Q. When did you start looking at cyber security in the fuel retail sector?

A. The petrol station topic is something I stumbled upon. When doing a workshop for general industries on how they should secure themselves I did some research for examples. I found vulnerable automatic tank gauges at petrol stations using special search engines where one can find

public devices that are unsecure. It's quite difficult to find unsafe devices due to the number of honeypots – systems that are meant to be found and hacked just to see what the attackers do. These kind of searches are normally done on a global basis. The product that I found was distributed all over the world including the U.S. and Europe.

Q. Based on your own research, how do you find the level of security of the fuel retail industry compared to others?

A. I don't have all the evidence to answer that question. In my experience, there are different types of organizations. Digital organizations that have digital services as their core business; they are usually aware of their security and IT risks. There are industries that have high standards due to legal requirements such as banking and health. Others are aware of their situation due to the large quantities of data they handle, like a hotel chain. Most of the others have no real digital presence and are often not aware.

Q. The gas station and convenience store industry is rapidly adapting to new technologies and becoming more and more connected. What do you think retailers should be on the lookout for?

A. The problem with most classical industries is that they have evolved in the last decades with serial communication, missing authentication as nothing was connected; there was no need to secure it because you had to go there, cut a cable, put a box and then you would have access to it. As technology evolves and the benefits of interconnecting systems are clearer some take the step of interconnecting all stations without looking at the risks. As fuel companies do not have the know-how in digital business they need to rely on companies that do. They are very dependent on their suppliers. If a supplier produces a network card for a gas station they need to be careful and put it behind a firewall, for example. That's the industry part.

A very important thing is that they follow the rules of classic IT security measures - having an antivirus system, mail security system, segregate payment systems. These players have the traditional issues around Windows, emails, mobile phones... Plus the industry part. Systems should be segregated.

Q. Some retailers in charge of a smaller network of sites may not think they have to invest in an IT consultant or a secure system.

A. It is an easy calculation to make. A marketing agency with 200 employees was hit by a ransomware campaign and could not work for two weeks – you have to calculate how much does it cost to have that many people not working. If the average employee costs €3.000 per month, €150 per day, for 200 employees that would be paying €300.000 for two weeks of non-working capabilities. If you add penalties for not being able to deliver fuel or some goods expire, you can add that to the total costs. Calculate the damage and divide it by 10 – that can be the amount to invest in security.

Q. If you were a hacker looking to penetrate a fuel retailing network, what would you be

looking for and how could you disrupt it?

A. From an attacker perspective it's always about what I want to achieve. Most attackers do it just for fun. Going back to the automatic tank gauges we found on the Internet, many attackers just manipulated the names of the fuel to show they were there. Often you should not expect a lot of damage from them. Then there are criminals in search of money, the classic ransom attack. They look to disrupt the service to get a ransom. This is something that can be done at scale – that's why it works. One ransomware can be sent to a million recipients – some will click, others won't. At a country level, we can look at incidents such as the one in Ukraine for example, where hackers caused a blackout. They could modify systems on the Internet so that site operators and fuel depots won't be notified when storage is low. You can have political hacking, like a radical environmental group or a country.

Q. So you are a retailer and you receive a ransomware infection. What steps should they take?

A. Hopefully they would be a little prepared for such an attack. Ransomware hits that person who clicked the wrong link. It can happen, and it will happen. Almost every company has suffered this kind of attack. One infected computer is not a problem. If the virus can spread in the internal network, and there is no segregation, his colleagues will probably be affected. If possible, the company should have segregated their networks and patched their systems. It is a good idea to get in touch with a security company. Know who can help you. As an individual, what you can do in case of ransomware (encryption of a device) is that if you notice that something is being encrypted, shut down the computer. But you will definitely need help from experts.

Q. The petrol stations of the future are seen as mobility stations that will include a wide range of services including delivery services with drones, autonomous vehicles, bike sharing... All these services will be heavily connected and will make the challenge only bigger.

A. The challenge will certainly be bigger as the exposure increases. This is where the responsibility of the suppliers comes in. Buying cheap components from far away that are produced in mass could lead to millions of IoT devices being compromised because of one security vulnerability. Cheap can come with a lot of risk. Suppliers have to make sure they have an update cycle, security audits, fast reaction time to reported vulnerabilities... The manufacturers of those components are also responsible for segregating components from each other. It should now be possible to activate a car's breaks by infiltrating its media system. There should be a clear and even physical segregation between such components. We should only allow connections that are really necessary.

Interview by Oscar Smith Diamante

