19.11.2019

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Germany
http://www.pilz.com

Press Message

Pilz stands defiant against major cyberattack and sees restructure as an opportunity - “Cybercrime is a serious threat to our country”

Ostfildern, 19.11.2019 - **In mid-October Pilz GmbH & Co. KG became the target of a major cyberattack. Server and communication systems belonging to the Ostfildern-based automation company were affected worldwide. After four weeks the company is drawing some initial conclusions: Pilz has overcome the attack; production and customer service have been re-established. Overall the family business is emerging from the attack stronger. What’s more, the company is speaking out about the gravity of the threat level.**

On 13 October the monitoring systems on Pilz's web servers recorded suspicious activity, which was identified as a hacker attack. Immediately after the onset of the attack, Pilz switched off all the company’s networks and servers to prevent a potential proliferation of the attack, both within the company and externally.
However, the perpetrators had already used an encryption trojan, known as ransomware, to attack the worldwide server and encrypt some of the data.

No further proliferation of the attack

Within a few hours of the attack Pilz had notified the authorities and lodged a complaint. “With regard to the attack, we are in the best of hands with the investigating authorities. However, we are not allowed to say very much about the incident itself, so as not to jeopardise the ongoing investigations. However we can say this much: no customer or supplier data has been stolen and no viral proliferation of the attack has been identified. That’s good news!”, reports Thomas Pilz, Managing Partner of Pilz.

In the first few days the company used agile methods to get organised using whiteboards and secure messaging services. Working groups were formed and priorities were established together in consultation. Even as the attack was being countered, forensic experts were painstakingly checking which areas of the network had been affected and were cleaning the data. Step by step the company is getting its IT infrastructure back into operation. However, it will be some time before the usual level of full IT services is once again available to all staff.

Customer care the number one priority

“The number one priority is to support and supply our customers to the usual level of quality”, explains Susanne Kunschert, Managing Partner. Production at the European sites is now running at the same level as before the attack. For the time being, production and logistics are working additional shifts to guarantee deliveries. Customer Support is in direct contact with customers across the world.

The company also believes that the current situation provides opportunities to strengthen the company – and not only with regard to the IT: “The last few weeks have shown: the technology may fail, but the solidarity and engagement of the people and their willingness to resolve problems together have carried us through. We are positive as we look to the future.”

Sharing experiences and raising awareness

Kunschert added this: “The current wave of attacks against us and many other companies clearly demonstrates that cybercrime is increasingly becoming a serious threat to peace and prosperity in our country. We must all make a great effort to ensure that this type of organised criminality is given greater attention and that companies, associations, authorities and politicians work more closely together in future to ensure that other companies and institutions are spared what we went through!”

The target of the cyberattacks at Pilz was the company’s IT systems for “office communication”. However, the automation company supplies products and solutions in the field of safety and security that serve to protect human and machine (machinery safety) and protect plant and machinery from unauthorised access or manipulation (industrial security). As a safe automation company, Pilz will use the experiences from the current cyberattack to expand its existing expertise in the field of safety and security and share this with its customers.

Caption: *Four weeks after the cyberattack the Pilz GmbH & Co. KG is drawing some initial conclusions. (Photo: Pilz GmbH & Co. KG)*

You can find texts and images at www.pilz.com also for downloading. To go directly to the relevant internet pages in the press centre, enter the following Web code in the search of the home page.: **215276**

Pilz in social networks

In our social media channels we give you background information concerning the company and the people at Pilz, and we report on current developments in Automation Technology.

 https://www.facebook.com/pilzINT

 https://twitter.com/Pilz_INT

 https://www.youtube.com/user/PilzINT

 https://www.linkedin.com/company/pilz-safe-automation-australia-

Contact for journalists

Tony Catterson
Press contact
+64 9 6345350
office@pilz.co.nz