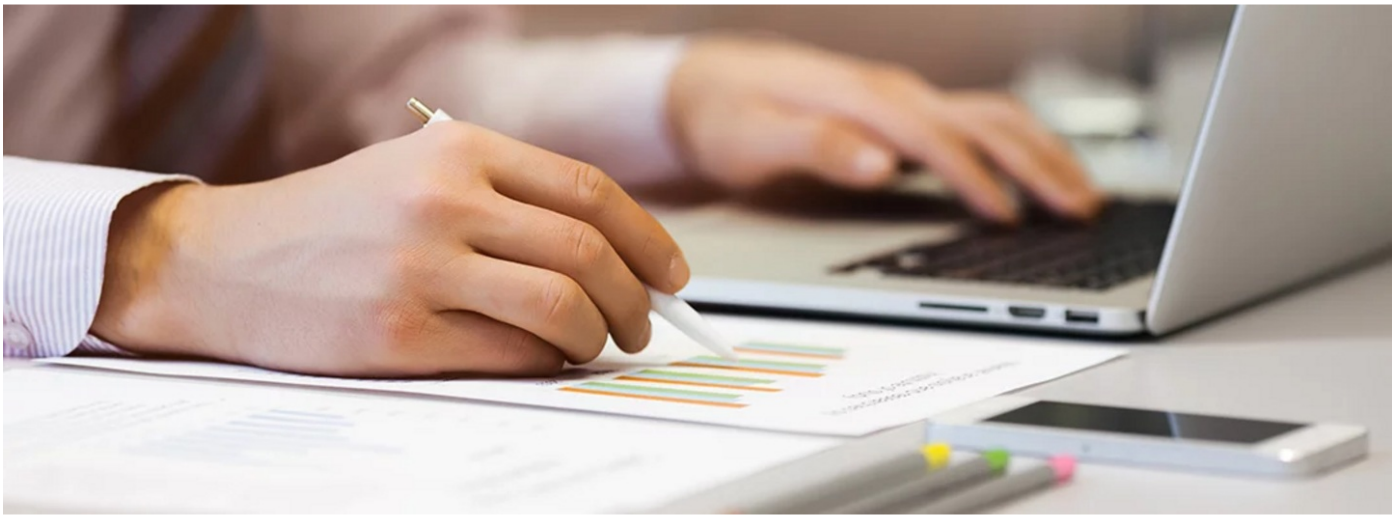

G+D Mobile Security solution provides protection against WannaCry and similar attacks

2017-05-16 Giesecke+Devrient

Munich, May 16, 2017 – Since last Friday, the ransomware "WannaCry" has attacked more than 200,000 computers in 150 countries and caused enormous damage. Like in previous attacks e.g. with Stuxnet, WannaCry was using a vulnerability within the system of unpatched or unhardened Windows computers. Industrial facilities and equipment without up-to-date IT security patch management are especially at risk: even if patches are already available as in this case, they are often not being installed in a timely manner. The Secure Industrial Visibility (SIV) solutions portfolio by G+D Mobile Security would have helped preventing the spread of WannaCry and thus considerably limited the resulting monetary damage.

In most cases, ransomware is being downloaded unknown to the user via manipulated email attachments or websites. If undetected, the ransomware can spread into the entire IT system. The risk of such an infection is especially high in industrial facilities as they typically do not use anti-virus software.

However, after the initial infection by ransomware, the affected system is changing its communications behaviour. The worm might for example conduct port scans, use uncommon network protocols or send information to conspicuous web addresses.

This is where the G+D Mobile Security SIV solution comes in: The Anomaly Detection System (ADS) developed by G+D detects and reports abnormal system behaviour. It will even detect it when the ransomware was previously unknown as the ADS is self-learning and does not require any signature updates.

The spread from the initially infected system to other computers, equipment and devices can now be effectively prevented by “Active Cyber Protection” and common IT security systems.

Amongst others, SIV can disconnect systems which are unable to follow the IT security life cycle themselves, such as machines. These systems mostly do not follow any security-by-design rules and are therefore vulnerable to a broad extent. SIV minimizes this attack vector and translates obsolete unencrypted protocols to the most recent communications standards including optional encryption. Dr. Christian Schläger, Head of Cyber Security at G+D, confirms the solutions’ effectiveness: “SIV successfully prevents the scanning of open ports as a point of attack and effectively hides the equipment’s operating system from outsiders. The solution therefore prevents attacks like WannaCry or their spreading inside IT systems.” Furthermore, inactive system ports are being sealed off.

For many years, the G+D Mobile Security Secure Industrial Visibility (SIV) portfolio has been offering security in high security areas to protect industrial equipment and industry 4.0 applications. With a dedicated service offering for Managed Security in the medical and industrial IoT sector, G+D Mobile Security brings their expertise to a wide range of industry customers. Current SIV customers can be found in the health and automotive industry, the construction and mechanical engineering sector as well as the production industry.

About G+D Mobile Security

Giesecke+Devrient (G+D) is a global security technology group headquartered in Munich, Germany. Founded in 1852, the Group has a workforce of 11,300 employees and generated sales of approximately EUR 2.1 billion in the 2016 fiscal year. 72 subsidiaries and joint ventures in 32 countries ensure customer proximity worldwide.

G+D develops, produces, and distributes products and solutions in the payment, secure communication, and identity management sectors. G+D is a technology leader in these markets and holds a strong competitive position. The Group’s customer base mainly comprises central and commercial banks, mobile network operators, business enterprises, governments, and public authorities. For more information, please visit: www.gi-de.com.