No.48
February 23rd 2021

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UN-SPONSORED**

A New Strategy for Telekom Security

Last week, T-Systems International GmbH (T-Systems) held a business update for industry influencers led by Thomas Fetten and Thomas Tschersich, CEO and CTO of affiliate Deutsche Telekom Security GmbH (Telekom Security).

- Telekom Security is focusing on the Central European markets of Germany, Austria and Switzerland. M&A activity may even prioritize the U.S. before the big European markets like France and the UK.
- Telekom Security is making a big push into converging IT and OT security via a new Magenta Industrial Security service managed out of its SOC.
- The company's value proposition is refreshingly pragmatic. It's focused on getting the basics right with a balanced emphasis across the whole of the NIST framework.

An Independent GmbH with 1,600 Employees

Telekom Security GmbH was carved out as an independent subsidiary of Deutsche Telekom AG in July of last year, shortly after the parent company completed the merger of T-Mobile and Sprint. Giving Telekom Security more flexibility is one of a series of measures designed to turn around T-Systems' poor financial performance. This has seen T-Systems headcount reduced by around 9,500 employees since the end of 2019 to 28,600 last September. For the first nine months of 2020, T-Systems losses grew to €618 million on revenues of €3.1 billion.

Up until fairly recently, Deutsche Telekom had the goal of becoming the pan-European leader in cyber security.

Today, Telekom Security lags its European telco peers in terms of some key metrics. BT Security and Orange Cyberdefense each have annual revenues estimated to be in excess of €750 million. BT claims a cyber security headcount of more than 3,000, Orange claims more than 2,500. Telekom Security will only say that its revenues are "far above" €250 million (growing in double digits). The company's headcount has reached more than 1,600, up from 1,000 at the beginning of 2017.

The Central European Leader Rather than the Pan-European Leader

Up until fairly recently, Deutsche Telekom had the goal of becoming the pan-European leader in cyber security. Under the leadership of Telekom Security's new CEO, Thomas Fetten, the former CEO of Orange Cyberdefense, the geographical focus of Telekom Security's strategy has been narrowed to allow a more concentrated focus.

While Telekom Security continues to serve customer sites throughout Europe and internationally – it has SOCs in Singapore, Brazil and Mexico, for example – the goal of becoming the pan-European leader in cyber security has been firmly put on hold.

The priority now is to double down on the 'DACH' markets of Germany, Austria and Switzerland. These are home to the core target of medium sized companies – the 'Mittlestand' – that often have a global presence and cyber security requirements that are both stringent and complex. Critically, many of these companies also have limited in-house cyber security expertise. Telekom Security is contributing to T-Systems' drive to differentiate here in the context of a common business culture of very stringent privacy requirements across the DACH region.

T-Systems continues to believe that positioning itself as a trusted European cloud provider against US-based giants like Google and AWS can deliver positive results. The strategy hasn't delivered as well as hoped but the belief is that the value proposition to businesses will improve following the so-called Schrems II ruling of July 2020 that affects the transfer of personal data out of the EU to third countries, notably the U.S.

If there are to be cyber security acquisitions in other European markets like France and the UK, management's message is that it won't be for at least a couple of years. In light of the Sprint merger, HardenStance wouldn't be surprised if Telekom Security were to focus any M&A activity on the U.S. before it gets round to France and UK.

End to End Portfolio and Positioning

Telekom Security's portfolio and market positioning will continue leveraging the 'Magenta Security' brand and remains firmly rooted in supporting the original NIST Cyber Security framework end to end. This spans all five identification, protection, detection, respond and recovery domains of the NIST Framework. This is important because while the rise of Secure Access Services Edge (SASE) in cyber security thinking may serve to counter it somewhat, the positioning of some leading MSSPs has edged towards greater emphasis on Managed Detection and Response (MDR) in the last couple of years.

If there are to be cyber security acquisitions in other European markets like France and the UK, management's message is that it won't be for at least a couple of years.

Telekom Security is pointedly maintaining balance in its messaging around the importance of all five domains. Management emphasizes continued investment in professional services to fulfil the advisory component of identifying an organization's vulnerabilities at the outset of a customer engagement - and on an ongoing basis. The company will also continue supporting a variety of different sales and delivery formats, albeit the goal is to drive as much business as possible in the direction of software sales and especially managed security services.

A pretty useful guideline for cyber security best practice consists of:

a) avoid doing stupid things that you should not do;

b) do all the simple things that you should do;

c) don't try doing additional clever things until you have a process for assuring you are consistently abiding by (a) and (b).

Whereas a lot of vendors – and some MSSPs – have a tendency to like selling complex, high margin technology, Telekom Security's essentially pragmatic pitch is refreshing. For example, use of 'AI' in cyber security got one single, cursory, mention during the recent influencer briefing - and that only arose in the context of a response to an audience question. This no-frills, 'get the basics right, first' approach is reflected in the customer challenges Telekom Security chooses to prioritize in its communications, hence by extension the solutions it offers customers in the first instance.

The first four priorities cited by management are recognizable as key by pretty much any cyber security provider anywhere in the world:

- **Patching Updates**. Probably compounded by the SolarWinds attack, Telekom Security reports that many customers continue to expose themselves to unnecessary risk because they persist in believing that they are at greater risk from allowing patching updates than they are from delaying them.
- **Log Visibility and Investigations**. Many customers collect volumes of logs but lack either the time or the expertise to investigate them, leaving threats to dwell in their environment undetected.
- **DDoS Attacks**. Via its access to Deutsche Telekom's backbone network, Telekom Security reports seeing a couple of thousand DDoS attacks of 10 Gbit/s or more every month – enough to take many customer data centres off-line. It sees many organizations being blackmailed as a condition of allowing normal service to be

restored. Here the company seeks to differentiate itself by way of being the affiliate of Deutsche Telekom, hence much more directly engaged than most cyber security providers in combating cyber-crime. The company points to its key role in the recent taking down of the Emotet botnet - and how it can leverage intelligence from such activities to customize relevant insights for specific types of customer.

- **Supply Chain Security.** Again, the Solar Winds attack has given new urgency to an area that was already a priority in Telekom Security's portfolio.

On a lesser scale, Deepfake video and audio attacks is one area Telekom Security elevates in importance above what HardenStance routinely sees from a large MSSP.

Converging IT and OT for Industrial Security

Management anticipates some, albeit limited, growth in IT security budgets due to the economic headwinds impacting businesses arising from the pandemic. The company is nevertheless a lot more upbeat about the spending outlook for OT security and on converging IT and OT security in particular.

This is a key growth segment for Telekom Security, aligning well with many of the industrial sectors that its core Mittelstand customers operate in. In this spirit, the company announced last week that the new Magenta Industrial Security service went live, offering protection of connected industrial machines against cyberattack.

Fake Audio, Fake Video and Deepfakes

On a lesser scale, Deepfake video and audio attacks is one area Telekom Security elevates in importance above what HardenStance routinely sees from a large MSSP. Deepfake videos have not reached full maturity yet but even rudimentary and intermediary variants are causing substantial harm. The recent fake video of U.S House of Representatives Speaker, Nancy Pelosi, appearing drunk – viewed more than two million times - was created just by slowing the video down.

Telekom Security has seen voice and audio manipulation techniques being used to trick employees, such as when someone who sounds very much like their CEO or CFO calls them with urgent instructions out of the blue.

Telekom Security's Channels to Market

Telekom Security serves customers through four channels – directly; via Telekom Deutschland GmbH; via Deutsche Telekom Business Services (DTBS); and via T-Systems International. ■

More Information

- T-Systems Targets UK Security Market (September 2019)
- "Cyber Security Innovators": Deutsche Telekom (March 2018)

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, OASIS, ETSI and TM Forum. www.hardenstance.com.

To receive an email notification whenever HardenStance releases new reports in the public domain, register here (there are only four fields): Registration Link

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, non-infringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.