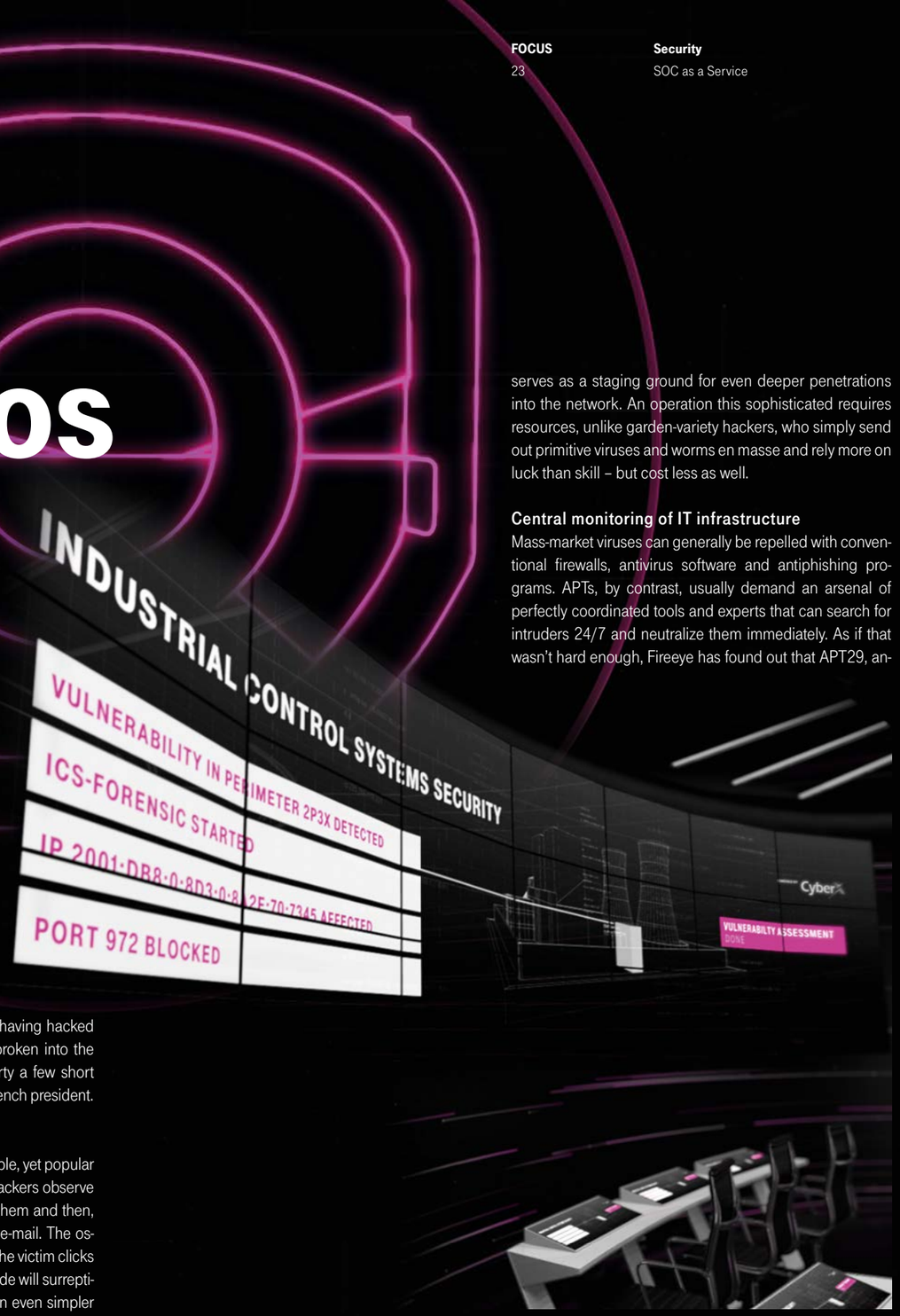
Where pros fight pros

They creep up, wait patiently and pounce undetected. Advanced persistent threats (APTs) worm their way into IT systems, siphon off data and paralyze entire organizations. To shield themselves from this latest generation of highly professional cyber attacks, more and more organizations are turning to external security operation centers. One provider who offers SOC as a Service is Deutsche Telekom.



Photos: T-Systems

COPY —— Roger Homrich

They're called Operation Pawn Storm, Office Monkeys or Fancy Bear. But only their names are fancy. They themselves are cunning, ruthless and willing to inflict sleepless nights on security experts. They work as burglars-for-hire, cyber mercenaries who target and attack corporate infrastructures for their clients. The attack begins when malware slips into a network unnoticed. The program spreads stealthily, skims off data and sends it back to the attackers and their clients. The typical cyber spy remains undetected for 208 days, according to estimates by the Federal Office for Information Security (BSI). But that's only an average. Many stay under the radar for much longer. "The current record, according to our findings, is five years," said Dr. Alexander Schinner, an IT forensic analyst at T-Systems who tracks down Internet attackers.

APT28 is a hacker collective that has been stalking targets for years. Also known as Fancy Bear, its members strike wherever clients send them – if the price is right. These Russian cyber soldiers allegedly breached the Democratic National Committee's servers during the US presidential election campaign. APT28 is also suspected of having hacked the German Bundestag in May 2015 and broken into the e-mail accounts of Emmanuel Macron's party a few short days before the recent run-off elections for French president.

Beware of e-mails from "friends"

Cyber spies use various techniques. One simple, yet popular method is known as "spear phishing". The hackers observe their targets, learn whatever they can about them and then, one day, send them a seemingly innocuous e-mail. The ostensible sender: a friend or family member. If the victim clicks the enclosed link or attachment, malicious code will surreptitiously install itself on the target computer. An even simpler trap: the malware resides on an infected website, where it awaits unsuspecting visitors, like a tick in tall grass. Or, cyber spooks may wriggle through published network security holes that aren't patched quickly enough.

Installing the code is only the first step. "APT28 employs a suite of malware with features indicative of the group's plans for continued operations," according to a Fireeye report. The hackers set up a virtual office that serves as a staging ground for even deeper penetrations into the network. An operation this sophisticated requires resources, unlike garden-variety hackers, who simply send out primitive viruses and worms en masse and rely more on luck than skill – but cost less as well.

Central monitoring of IT infrastructure

Mass-market viruses can generally be repelled with conventional firewalls, antivirus software and antiphishing programs. APTs, by contrast, usually demand an arsenal of perfectly coordinated tools and experts that can search for intruders 24/7 and neutralize them immediately. As if that wasn't hard enough, Fireeye has found out that APT29, another Russian cyber espionage outfit, has also been employing "domain fronting." This technique disguises the malware's sender address, making it significantly harder for victim organizations to identify malicious data traffic.

Until recently, only large companies had the funds to professionally orchestrate their cyber defenses. This is a big project: it involves building security operation centers (SOCs) that monitor central IT resources and data for signs of compromise and manage the responses to IT threats. "SOCs resemble command centers where security experts track 'enemy activity' worldwide on big screens, investigate system alarms and take immediate action as needed," explained René Reutter, Vice President IT Security Engineering & Operations and the head of the Deutsche Telekom SOCs.

Carefully coordinated tools

In fulfilling their mission, defense teams employ a broad range of security tools that automatically scan the IT systems under their protection. The systems interface directly with the SOC so that all data traffic can be monitored and analyzed. However, SOCs are costly to build, operate and crew with highly trained specialists in a wide variety of roles. That's why more and more companies are sharing these costs and turning to externally managed SOCs.

Thanks to cloud technology, service providers like Deutsche Telekom can offer "SOC as a Service": instead of operating a dedicated security operation center for each client, they can protect multiple clients simultaneously with a single SOC.

As a result, Deutsche Telekom is giving Germany's SMBs – which represent nearly half of the world's hidden champions – access to the level of security that until recently was the exclusive preserve of major corporations. It has also eliminated the two biggest obstacles to mid-market enterprises' own security ambitions: not only can they exit the war for high-priced talent, but they also don't have to invest in expensive equipment of their own. Given the persistent shortage of skilled labor, Frank Luzsicza, Division Head of ICT & Business Solutions at TÜV Rheinland, believes that "having a competent external cyber security partner that you trust will become one of the most important success factors for a company's security."

Driven by KRITIS and IT Security Act

"SOCs are not really new," said Rüdiger Peusquens. "However, the German IT Security Act and the growing sophistication of cyber attacks have only now stirred up interest in the topic," noted the head of Deutsche Telekom's Cyber Defense Center, responsible for protecting Deutsche Telekom as a critical element of infrastructure. The KRITIS Regulation, which implements the IT Security Act, recently went into effect. Now, companies in the IT, food, utility, finance, traffic, transportation and telecommunications industries have to take special precautions to keep their IT systems secure and available.

The Security Operations Center in Bonn and the Deutsche Telekom Cyber Defense Center plan to work together to centrally monitor Deutsche Telekom customers' IT infrastructure starting in the third quarter of this year.

Only recently, in March 2017, a large energy company entrusted Deutsche Telekom with handling its threat and vulnerability management as well as state-of-the-art analytics for smoothly operating its infrastructure. "An SOC can centrally aggregate and analyze information from all of the process layers in an organization. That has tremendous significance," said Dirk Backofen, Head of Telekom Security, the new Group business unit. "You need this depth of information in order to properly manage your operating environment and its various security levels." But that also requires protecting each layer of the customer's business with a suitable security solution and having the know-how to steer the customer to the right combination of offerings for its use cases.

The depth of experience needed just to select the right technologies and use them properly is one of many reasons for rising worldwide demand for security cyber defense orchestration. Starting this autumn, Telekom Security's new SOC in Bonn and the Deutsche Telekom Cyber Defense Center will work together to serve that demand.

Prevent, detect, respond

The defensive and offensive technologies required by SOCs may resemble a chaotic patchwork, but they quickly resolve into an organized structure when an SOC's job is broken down into three levels: prevention, detection, response. In other words, how can I secure an organization in advance? How can I tell if my firewall – as often happens – lets ransomware, APTs and other malware into my network, and intrusion prevention or advanced threat protection solutions have to kick in automatically? And who or what will respond to infected systems on the fly as quickly as possible 24/7/365 – whether remotely or on-premises? Perhaps to quarantine malware or uninstall an infected computer. And these are merely the simpler aspects of Telekom Security's incident response retainer service. Equally important are the 'who' and 'what' questions: What exactly happened? What data was exfiltrated? Did it include trade secrets? Where did the data go? There aren't many experts in Europe who have the forensic skills and experience to answer these questions; over a dozen work at Deutsche Telekom.

Security for industrial systems

Industrial networks and interconnected computers, instruments and control systems can be highly vulnerable to attack by APTs. "Plants frequently run on obsolete technology with no way to ward off cyber attacks. The systems just aren't designed to be used in a network," said Bernd Jäger, an expert in industrial control systems security (ICS) at Deutsche Telekom. "Conventional IT security systems like firewalls don't work in these types of environments, and knowledge of cyber security for industrial networks is often rudimentary at best." To fill this gap, Deutsche Telekom has expanded its portfolio of security partners to include companies that have developed security solutions tailored to industrial users. These ICS security products focus on reducing detection times in industrial networks and helping managers make appropriate decisions by instituting automatic protection and response mechanisms when and as needed. "These solutions can also be part of a managed security operation center," explained Reutter.

Clearly, SOCs can have a tremendous impact, as an example from the world of sports shows. An SOC might have saved the World Anti-Doping Agency (WADA) more than a few headaches. Fancy Bear visited the WADA databases multiple times – as its members gleefully admit. "Greetings, citizens of the world," proclaims their start page at https://fancybear.net/. "We stand for fair play and clean sport. We are going to tell you how Olympic medals are won. We hacked World Anti-Doping Agency databases and we were shocked with what we saw." Sometimes hacking can be useful, too.

reutter@t-systems.com
www.t-systems.com/telekom/security-operation-center
www.t-systems.com/solutions/cyber-security

"SOCs resemble command centers where security experts track 'enemy activity' worldwide and take immediate action as needed."

RENÉ REUTTER, head of the Telekom Security Operations Center

Photos: T-Systems

INTERVIEW

"We can and will deliver."

Head of Telekom Security, Dirk Backofen, about how customers benefit from a European SOC landscape, the boom in the market for managed security services (MSS) and the "zero impact" approach to protecting companies from cyber attacks.

COPY — Thomas van Zütphen

Mr. Backofen, the market for SOCs and other managed security solutions is booming. Why is that?
Customers don't have the resources to keep up with the rapid evolution of new technologies and the sheer number of solution providers in the security market. Hackers, however, will quickly adopt new technologies for cyber attacks. That means that companies need a strong partner that is well versed in many different industries so it can offer as complete a cyber security shield as possible. Deutsche Telekom is this strong partner. We can deliver. For 20 years, we've been protecting not only ourselves, but large swathes of the German private and public sector as well.

How will consolidating all of the Group's security resources in Telekom Security change things?
Even the tiniest device now contains a super computer and all these devices are linked together. This is a world of "everything connectivity". We need "everything security" to match it. That's no small feat. To reach this goal, we are pooling the expertise of all our specialists – currently numbering 1,200 strong – into one agile, high-performing business unit and thereby investing directly in our customers' security. Deutsche Telekom spends about 250 million euros each year just protecting itself with best-in-class security solutions. This figure goes up every year. This demands tremendous expertise, management and organizational talent. It only makes sense to let our customers share in the benefits from this investment, too.

Dirk Backofen, Head of the Telekom Security corporate business unit

So what is Telekom Security's specific approach?
Our goal is to make security simple for customers. To make it convenient, practical, understandable – and yet highly secure. We believe in zero impact. We can never prevent cyber attacks, but we can keep them from having an impact.

You've touched on the problem: for many companies, security isn't just complicated. It's also expensive. What's your answer to them?
That it's not true! Obviously, security costs money. But it's wrong to treat security as just another cost center. On the contrary, properly installed and orchestrated security systems will save money by avoiding much more expensive losses. That perspective reveals security to be a necessary, important investment. Deutsche Telekom CEO Tim Höttges had clear words of advice for managers asking about the best places to invest: "My fellow CEOs, when it comes to cyber security, don't listen to your CFOs. Listen to your nerds." I couldn't have said it better myself.

Back to the SOCs – why are you expanding the landscape of your security operation centers?
We already have a series of specialized SOCs in Germany, Hungary, Slovakia and South Africa. Starting this fall, our new, state-of-the-art SOC in Bonn, Germany will use the know-how of all the SOCs in the various Deutsche Telekom networks to proactively deflect attacks. This will be our first integrated Cyber Defense and Security Operation Center where Deutsche Telekom, as one client among many – and always pursuant to the agreed-upon SLAs – can benefit from the experience of our cyber security experts and threat analysts. One prime example is our use cases, for which we use a wide range of analytical procedures. That allows us to link threat intelligence with cognitive security technology. As a result, we can leverage artificial intelligence and data mining to roll out new services that stop malware from communicating. In other words, we always know what's currently en vogue in the hacker community and try to stay one step ahead of them when it comes to our customers.

dirk.backofen@t-systems.com