To Stop Cyber Attacks Targeting Small and Medium-Sized German Businesses case study

When it comes to protecting small and medium-sized businesses (SMBs) from cyber attacks, smart managed security service providers (MSSPs) know that promoting security awareness is critical when delivering efficient and cost-effective security solutions. That's why BlackBerry MSSP partner abtis GmbH places so much importance on educating its SMB customers about security best practices and explaining why adversaries consider them such attractive targets of opportunity.

Since it was founded in 2003, abtis has grown rapidly and now serves more than 1,000 SMB customers from its headquarters in Pforzheim, Germany. In addition to providing customers with BlackBerry endpoint prevention, detection, and

response
solutions, abtis hosts a wide array of Microsoft® cloud and application services, including Microsoft's complete suite of Mobility + Security (EMS) products.

Those Who Can Do Also Teach

According to abtis CEO and founder Thorsten Weimann, "Most SMBs in southern Germany think security means having a firewall and an antivirus application. They seldom have security budgets, chief information security officers, or even specialists responsible for managing cyber risks. Instead, we see teams of four or five generalists managing an entire IT infrastructure and supporting 500 employees or more."

Sometimes, abtis has to find creative ways to frame security issues in terms that SMBs more readily understand and appreciate. According to Thorsten, "We tell them to think about their data the way they think about their health. If they get sick, they can't go to work. It's the same thing with their data. If it gets encrypted by ransomware, they can't do business." Often, prospective customers don't approach abtis until after a ransomware attack is already underway. "When that happens, our first move is to neutralize the infection by deploying CylancePROTECT®,*" says Thorsten.

abtis prospects are often unaware that they could face significant financial penalties prescribed by German and European Union (EU) cybersecurity regulations if they allow private and confidential data to be exposed due to a breach. "We use ourselves as an example," says Thorsten. "We describe the rationale behind the investments we've made to comply with the Federal German Data Protection Act and the European Union General Data Protection Regulation (GDPR). This enables us to speak with authority when we recommend security solutions to our customers."

Deficits in security preparedness are not confined to the German marketplace alone. SMBs across the globe are being attacked more frequently and with greater impact than ever before. The Ponemon Institute reports[1] that the number of SMBs experiencing a data breach increased from 54% in 2017 to 63% in 2019, and that global cyber attacks targeting SMBs rose 20% since 2016. The impact of a breach may also be felt more acutely by an SMB than a larger organization. According to a report sponsored by IBM Research[2], data breach costs are much higher for SMBs ($3,533 per employee) than for large firms ($204 per employee)[3]. These higher proportional costs make it more difficult for an SMB to recover and resume operating than for a large firm with greater resources and deeper pockets.

MSSPs in the Cross Hairs

In recent years, MSSPs have also become high-value targets for cyber attacks. In July 2019, the BlackBerry Research and Intelligence Unit profiled Sodinokibi4, a new ransomware strain that infiltrated hosted environments and infected thousands of MSSP customers. The BlackBerry Cybersecurity Consulting Services team also observed another attack in which an adversary exploited an MSSP's remote support application to compromise a customer's environment, steal credentials, infect a domain controller, and disable the victim's antivirus.

"We're well aware that we're being targeted because of the access we have to our customers' data and networks," says Thorsten. In addition to CylancePROTECT and CylanceOPTICS®, abtis has also implemented multifactor authentication, identity protection, and more. "We're constantly tuning our defenses and monitoring our environment for early indicators of compromise," says Thorsten. "You can't be hacked yourself and still be a credible provider of managed services."

A Partnership Is Born

In 2017, abtis became dissatisfied with its legacy antivirus and began looking for an endpoint security solution that was more effective and easier to manage. "We were losing too many productive hours each week updating signature files and dealing with system performance problems caused by signature updates and intrusive scans," he says. "We were excited when we learned about BlackBerry's endpoint security solution at one of the tradeshow events we attended in the United States."

abtis finds the CylancePROTECT implementation process to be simple and straightforward. "The process of scanning, defining exceptions and then enabling security controls is both intuitive and logical," says Thorsten. "In my experience, vendors often overstate the capabilities and benefits of their products. I'm delighted to say that BlackBerry and its CylancePROTECT and CylanceOPTICS solutions continue exceeding our expectations."

A Winning Proposition for abtis and Its Customers

abtis offers two tiers of managed endpoint protection services. Managed Endpoint Protection is a cost-effective solution for smaller customers and includes a
deployment of CylancePROTECT. *Managed Endpoint Protection and Response* is abtis' premium product, adding CylanceOPTICS for AI-driven threat detection and response. "In both cases, we provide customers with 24x7 support from our Security Operations Center," says Thorsten.

abtis is so confident in its value proposition that it doesn't ask for long-term commitments or charge for the first month of managed services. During that time,
abtis deploys BlackBerry's agile agent technology to an initial set of customer endpoints, and fine-tunes CylancePROTECT security controls for malware prevention,
memory exploitation protection and script control. According to Thorsten,

"It's
essential for onboarding to proceed as efficiently and transparently as possible to build trust in our services and solutions. So far, we've had a perfect track record. Every prospect who has onboarded CylancePROTECT has become a paying customer."

Every human relationship requires mutual trust and loyalty to deepen and grow. The same is true for the partnership between abtis and BlackBerry. Says Thorsten, "We trust BlackBerry and its products. We wouldn't even consider recommending any other solutions for endpoint protection, detection, and response." He has also come to rely on BlackBerry to help grow abtis' business. "The BlackBerry partner team provides us with exceptional support," says Thorsten. "Whenever we ask, they join us on sales calls and provide speakers for our roadshow and customer events. BlackBerry has shown over and over that it really is committed to our success."