QUALITY. CHOCOLATE. SECURED.

Company: **Alfred Ritter GmbH & Co. KG**

Industry: **Food / Confectionery Manufacturing**

Country: **Germany**

Solution: **F-Secure Rapid Detection & Response Service; F-Secure Business Suite Premium**

Anyone looking for a chocolate paradise will hit gold in the idyllic small town of Waldenbuch, home to the headquarters and production facilities of Alfred Ritter GmbH & Co. KG.

This is the town where, in 1932, the legendary square-shaped chocolate bar that now enjoys cult status well beyond the borders of Germany was invented. Since 1960, the family business has concentrated exclusively on the square-shaped chocolate, with a wide product range anywhere from small chocolate cubes to heavy-weight 250 gram bars.

Ritter Sport is skilled at blending tradition with innovation with its global workforce of over 1500 employees that use state-of-the-art production technology and need to be able to rely at all times on fully functional IT. That is why the sensational cyberattacks in 2016 and 2017, which paralyzed countless production plants around the world, made the company's management stand up and take notice.

With around three million Ritter Sport chocolate bars leaving the production lines in Waldenbuch every day, it is not hard to imagine the catastrophic effect that a hacker-induced production stoppage would have on the company. Not only would such a scenario slowdown business processes, it would also have a considerable impact on costs. Indeed, the real and not merely theoretical nature of the threat was demonstrated to Ritter's management through the unfortunate experience of another chocolate manufacturer, whose production line was brought to a standstill for a whole week in June 2017 as the result of an attack.

LIFE IS LIKE A BOX OF CHOCOLATES

You don't know exactly what you will get. Although 99.9% of all security incidents are automated attacks involving spyware, ransomware, banking Trojans, self-replicating botnets, and so on (with endpoint security, email security and firewalls providing a very good defense), no technology can offer 100% protection against cyberattacks. This is particularly true of complex, targeted attacks, which, despite accounting for only 0.1% of the total volume, cause considerably more damage. Like most companies, Ritter Sport had no protection against this type of cyberattacks, as the focus of its security strategy was understandably on the most commonly occurring threats.

When your adversary is a human being, you don't know exactly what you will get and you cannot rely solely on computer technology. To detect intruders and respond rapidly, you need to supplement smart software with human expertise. Otherwise, the threats will only be identified weeks, months or even years later – with serious consequences for costs and reputation.

Ritter Sport saw this as the ideal moment to put an advanced threat monitoring system in place that immediately flags suspicious behavior in the corporate network. That's why they chose F-Secure Rapid Detection & Response Service (RDS). The analysts at the F-Secure's operations center deliver around-the-clock monitoring of Ritter Sport's IT environment to detect signs of security breaches, analyze suspicious activity in real time, investigate the results and filter out false positives. Within 30 minutes of confirming that an anomaly is an actual threat, the customer's IT team is alerted.

CRACKING HARD NUTS

The security measures were implemented at exactly the right time. When Ritter Sport was subjected to a targeted attack in November 2017, the F-Secure team flagged the incident in just nine minutes – well within the promised reaction time.

In another incident in March 2018, F-Secure was even able to sound the alarm within six minutes. The focus of the attack was Microsoft Office: a malicious macro had caused unusual behavior in the system. The sensors immediately detected the attempted intrusion and downstream analysts at the Rapid Detection Center were soon able to identify the anomaly.

In both cases, the cause was an email – a commonly used attack vector, as F-Secure's most recent Incident Response Report shows. More than a third of all digital incidents in the corporate world originate through phishing emails or malicious email attachments. The most frequent method is when attackers exploit software vulnerabilities. In 21% of the cases examined, this was the method attackers used to gain access to the company's infrastructure. In 34% of all cases, however, no vulnerability was required. The attack was carried out through phishing and malicious email attachments – a method that companies find difficult to contain.

A REFINED BLEND

Rapid Detection & Response Service swiftly detects advanced cyberattacks through a combination of artificial intelligence and an international team of threat hunters. The team investigates each incident and decides whether it needs to be reported. The IT security team at Ritter Sport are then notified of the serious incident by telephone, and not by email or text message. The experts work around the clock to monitor, analyze and evaluate attacks in order to initiate the right response at exactly the right time.

For some time now, the chocolate manufacturer has successfully deployed F-Secure Business Suite Premium to protect all of its PC systems and many Citrix terminal servers. The F-Secure's managed detection and response service was implemented at Ritter Sport by F-Secure's partner, BWG Informationssysteme. Just like in the first project involving Ritter Sport and F-Secure, the system administrator, Michael Jany, felt it important to choose a European manufacturer and German partner, both with strict "no backdoor" policies.

F-Secure Rapid Detection & Response Service now monitors around 1,000 connected endpoints at Ritter Sport around the clock, 365 days a year. To date, F-Secure has significantly outperformed its promise to detect and flag security incidents within 30 minutes. This makes it possible to immediately measure the return on investment (ROI). "This not only convinced us, the IT team, but also our CFO and the financial controllers," says Jany.

CYBERATTACKS: NO SWEET SURRENDER

"Thanks to Business Suite Premium and Rapid Detection & Response Service, our systems are now fully protected against all forms of malware and targeted cyberattacks. RDS has already done an amazing job on two occasions in just a few minutes," says Michael Jany, describing the success achieved since its introduction. "We are completely convinced that we have chosen the right solutions. What's more, we consider F-Secure's Rapid Detection & Response Center experts to be full-fledged members of our security team."

Cyber security experts monitor your environment around the clock

Max. 30 minutes from breach detection to response, as agreed in a Service Level Agreement

Direct return on investment through out-of-the-box ready Managed Service

How do you detect a sophisticated attack? You make use of the most advanced analytics and machine learning technologies. But that's not all. You've got to think like an attacker.

F-Secure's security experts have participated in more European cyber crime investigations than any other company. With our experts' fingers firmly on the pulse of the cyber attack landscape, you'll stay up to date with the latest threat intelligence.

F-Secure

Learn more at > f-secure.com/RDS