REDSOCKS
malicious threat detection

Case Study

RedSocks Security assists Yamaha Motor Europe in Compliance and Cyber Security

Motorcycle lovers worldwide get a look of recognition in their eyes when they hear the name 'Yamaha'. That is quite understandable, as the Japanese manufacturer has been a household name for 62 years when it comes to motorcycles. It is a dream come true for founder Genichi Kawakami. Under the motto "If you're going to do something, make sure that it's the best", he made sure that the Yamaha became synonymous with the ultimate engine technology.

Nowadays, Yamaha Motor is not limited to the design and manufacturing of motorcycles; the activities of the Group include the design and manufacturing of All Terrain Vehicles, marine engines, boats, wave runners, and even golf carts. These activities have resulted in revenues of 1,502.8 billion yen (about 12.59 billion Euros) and a profit of 63.2 billion yen (over 529 million euro) in 2016. Yamaha established its European headquarters in 1968, including a major distribution center, in the Netherlands.

The Situation

The Japanese manufacturer has fifteen physical locations in Europe, including two factories and five large warehouses. The European headquarters of Yamaha Motor, housed in The Netherlands, acts as hub for the region.

"That will also apply largely to our IT infrastructure. The centralization of the European IT of Yamaha Motor is now in full swing, "said Sjoerd Nijmeijer, Department Manager IT Infrastructure Information Systems at Yamaha Motor Europe. The two data centers that host various internal applications and various websites are located in the Netherlands. The 'regular information security' is of course of great importance to Yamaha Motor. But the recording of incidents, such as abnormal network traffic, also has a high priority.

However, the existing tools for that fell short, which was a detrimental issue considering the fact that the company has to adhere to strict regulations, such as the Japanese Financial Instruments and Exchange Law (also known as J-SOX), and also the GDPR in Europe. Yamaha Motor Europe decided that they needed a more pro-active cyber security solution to tackle that challenge.

The Solution

"When I started working for Yamaha in February 2016, the company had recently decided to use the Malicious Threat Detection (MTD) solution offered by RedSocks Security. The reasons for choosing the RedSocks Security MTD? It was primarily due to the fact that this solution offers great monitoring and logging capabilities. And, last but not least: it is a solution that's relatively easy to implement", says Sjoerd Nijmeijer.

The Implementation

The RedSocks MTD Appliance was delivered to Yamaha Motor Europe in the end of February 2016, where it was installed in the main data center.

Sjoerd Nijmeijer: "After the physical delivery, it took us only a few days to implement it." The extremely short installation and tweaking time is inherent to the design of RedSocks MTD, he explains: "It is first of all a matter of good preparations. And secondly because there are no major changes required in the organization or IT infrastructure. That made it very easy to implement."

The Benefits

The Malicious Threat Detection solution has been active for over a year in the data center of Yamaha Motor Europe. "To complete satisfaction", says Sjoerd Nijmeijer.

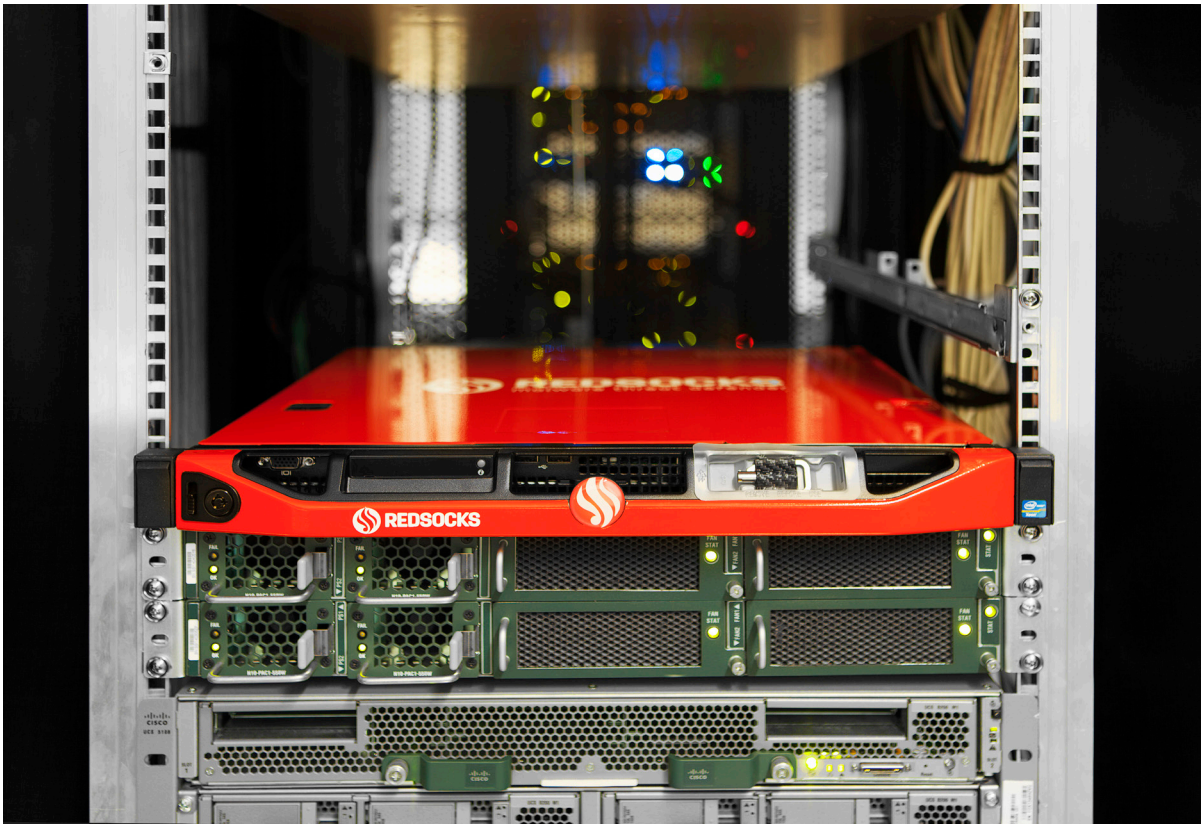
"The MTD has even 'saved' us twice. Once it sounded the alarm due to suspicious network behavior - strange DNS queries to be exact. It turned out to be caused by an infected mail server in our Swedish website. Thanks to the MTD we had that resolved before any harm was done.

The second time the MTD proved to be valuable, was when it detected a crypto locker infection on a laptop of one of our employees in the Netherlands. That is always annoying, but the damage was limited by the early notification of the incident by the MTD, and the fact that we have a good backup strategy for our endpoints. The Malicious Threat Detection solution really proved its worth on both occasions", says Nijmeijer.

The RedSocks MTD is also helpful in other areas, says Nijmeijer: "It makes the IT department of Yamaha Motor Europe aware of certain, less desirable things happening in the network, for example: it alerted us when an external consultant tried to access the internet using a TOR browser. That does not yield an immediate danger, but it is strange behavior considering the fact that often botnets are controlled via the TOR network.

When we asked the consultant about his browsing activities, he was surprised: 'Oh, can you detect that?'

Our answer was simple: ***Yes, we can***."



The Future

Today, Yamaha Motor Europe is very pleased with the Malicious Threat Detection solution of RedSocks Security. Does Sjoerd Nijmeijer have anything on his wishlist regarding the MTD road map? “If I have to mention something, then it would be the connectivity and interfacing with other systems. I’d like to see some extra functionality in that area.”

Does Sjoerd Nijmeijer anticipate deployment of additional MTD Appliances in the future?

“Not yet. The centralization of our European IT infrastructure is still in an early stage. One of the possible scenarios is that at some point in the future we will opt for a centralized, Europe-wide internet access. Then there may be a reason to consider deploying multiple MTD Appliances. “

RedSocks Security

RedSocks Security is specialised in detecting suspicious network behaviour and combatting cybercrime. By combining Machine Learning, Artificial Intelligence and Cyber Threat Intelligence, RedSocks Security provides non-intrusive, real-time malicious threat detection solutions and incident response services. Our solutions are implementable within organisations of all sizes, and also serve as a tool of compliance to EU privacy legislation.

Laan van Nieuw Oost-Indië, the Hague, the Netherlands • Tel +31 (0)88 13 33 300
E-mail info@redsocks.eu • website www.redsocks.eu