REDSOCKS
malicious threat detection

Case Study

RedSocks Security solutions offers TUI Benelux real-time Breach Detection and Forensic Logging

The terms ‘holiday’ and ‘relaxation’ are synonymous with TUI. The listed German group is one of the world’s leading companies in the tourism industry, with a turnover of over 17 billion euros and a net profit of over 1.1 billion (fiscal year 2015/2016). TUI is not only a mayor player when it comes down to the financials. It also employs a substantial amount of people: 67,000 people worldwide and 2.500 employees in The Netherlands. Together, they ensure that each year approximately 20 million customers worldwide and 1,6 million in The Netherlands have the holiday of their lives.

The portfolio of TUI is extensive: from ‘ordinary holidays’ to specialist varieties such as corporate events and even sports travel. TUI is more than just a tour operator: it owns over 300 hotels in 30 countries plus a fleet of cruise ships (14 units), buses and planes (150 pieces, including 9 in the Netherlands).

TUI Benelux incorporates the Belgian and Dutch activities under one virtual roof. Three data centers (in the Dutch city of Enschede and in Ostend, Belgium) equipped with redundancy and approximately 160 IT staff are the backbone of the IT. “Like any other organization with a large number of customer transactions and dealing with sensitive data of customers, information security is paramount at TUI. Naturally all our endpoints such as PC’s and laptops have antivirus software installed and our networks and servers are protected with firewalls and other cyber security measures. Still, we found that we could do even better, “says Theo Kip, IT Risk and Compliance Officer at TUI Benelux.

“A recent update of the Dutch law on Personal Data Protection and in its wake, the obligation to report data leaks, gave us a specific and pressing argument to look for ways to improve on our current security logging options”, explains Kip. “During a visit to a trade fair, we met RedSocks Security. Their Malicious Threat Detection solution seemed to me an interesting option: it not only offered ‘inside out’ malware detection, but it also had the most comprehensive forensic logging capabilities on the market.”

The Solution

TUI Benelux decided in 2016 to have a Proof of Concept built by RedSocks Security. Theo Kip: "During the PoC, we worked closely with experts from RedSocks Security. During that time we evaluated the solution. And we had them add functionality. For example, we had any additional requests regarding the handling of alerts and assigning tickets to and documenting of incidents. That was addressed properly by RedSocks Security."

In September 2016 TUI Benelux decide to buy the MTO technology of RedSocks Security. Kip: "The Proof of Concept was very convincing. We ended up buying a total of three MTD appliances for our data centers in the Netherlands and Belgium." His colleague Ronny Tyink, Team Leader System Engineering Network TUI Benelux, explains why the hardware appliance was chosen:

"We have chosen specifically for the hardware appliance instead of the virtual machine version, as we didn't have VMware installed and configured at all of our locations. The appliance version has the added benefit of being able to work independently of VMware availability."

The Implementation

Due to the extensive Proof of Concept phase, the actual implementation of the RedSocks MTD appliances proved to be relatively simple and quick, according to Theo Kip. "In the end, we had RedSocks Security leave the appliances behind that we used during the Proof of Concept. That saved us as well as RedSocks security a lot of time and efforts. The hardware isn't the most important part of the RedSocks Security MTD technology. The cyber threat intelligence is, in my opinion, really the crucial part."

The Benefits

The RedSocks MTD solution has, since its implementation in September 2016, already proved their worth for TUI Benelux. Theo Kip explains: "For example, we received malware alerts when colleagues from Morocco and Switzerland with an infected laptop tried to connect with our internal network.

"Thanks to the RedSocks MTD technology and logging functionality we were able to see exactly who had a malware infection with which device at which location. It allows us to turn suspicion into certainty."

Looking into the Future

TUI Benelux has had good experiences with the RedSocks Security MTD technology, according to Theo Kip and Ronny Tyink. They therefore don't rule out the possibility that other TUI subsidiaries will have a good look at the security solution, Kip: "I have regular discussions with my European colleagues during meetings of the TUI Information Security Board. In it we discuss current affairs and we formulate the Information Security Policies for the entire TUI Group. That could be a good platform to bring the RedSocks MTD security solution to the attention of my colleagues."

Looking at the future, TUI Benelux doesn't have an extensive wish list for the RedSocks Security MTD solution. Theo Kip and Ronny Tyink can only think of two things: "We would welcome an addition to management capabilities. To be more specific, we'd like to have the status of an MTD-Probe displayed in the management dashboard. Those Probes are an essential part of the malware detection and therefore it is good to see whether they function optimally. As for our second wish: we would like see some additions to the forensic logging functionality. We now save the log files of the last four months. This adds up to a total of 500 GB in storage capacity. It would be nice if we could keep log files that went back more than four months and we'd love to have an automatic alert when more storage capacity is required for the log files."

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.