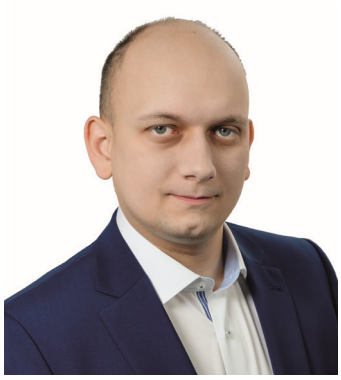
Your data and information are the most important assets. Keep your secrets secret



Andrzej Kaźmierczak

Technologies

MS AD RMS

MBAM

DLP

AppLocker (application white & black listing)

Country

Oman

Industry

Oil and production

Company Size

4 000

Duration

April 2015 – December 2016

Executive summary

Every day we are witness to cyber-attacks that lead to data breach and leakage. WikiLeaks, Snowden, WannaCry – these are today's examples of why a security strategy for data and information protection is crucial for every organization.

Description

Customer challenge

The customer is one of the biggest oil and production companies in Oman. They have approximately 4 000 employees and a lot information and data that should be considered confidential or secret and kept only for authorized personnel use. For our customer it was crucial to have a comprehensive solution that enforced information protection on different layers and in various potential scenarios (e.g. a stolen laptop, files copied outside the company, identity theft, running unapproved applications).

Project goals

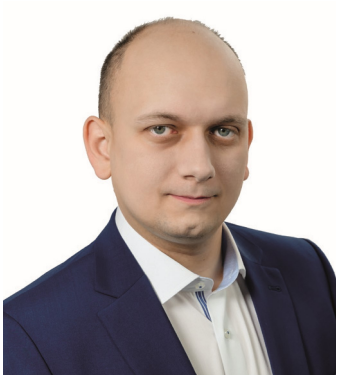
- To be compliant with ISO 27001 audit recommendations.
- To protect data and information wherever it is – at rest, in transfer and during processing.
- To deploy a comprehensive, easy to use and adoptable solution for sensitive data.

Solution

It was crucial to develop the client's security strategy and protect data on 600 computers from unauthorized access and potential data leakage. We have designed and implemented the following technologies:

- Active Directory Rights Management Services (to provide document encryption and apply policies to allow only authorized actions on documents – i.e. do not forward, do not print, do not edit).
- Microsoft BitLocker Administration and Monitoring (to help protect from data leakage in case of laptop thefts or losses).
- Data Loss Prevention (to apply the rules of sending sensitive information).
- Application white & blacklisting (to prevent unauthorized programs from running on the computers).

How to stay protected from the cyber-threats within?



Andrzej Kaźmierczak

Technologies

Advanced Threat Analytics

Country

Qatar

Industry

Government

Company Size

2 500

Duration

September 2016
– November 2016

Executive summary

The nature of modern attacks has noticeably changed in recent times. They are even more sophisticated and not designed to damage the infrastructure. Instead, attackers more often attempt to gain access to the network or employees' identities for profit. IT security has to keep up with these developments.

Description

Customer challenge

One of the government entities in Qatar was looking for a solution that would detect potential threats inside their IT infrastructure. Currently many security technologies are in place to protect it from the outside world, but once an attacker passes them, they may not be detected.

Project goals

To make sure that such a situation is unlikely, the client defined the following project goals:

- To protect the company from malicious attacks and to detect abnormal security issues and behaviors of users and devices.
- To reduce the risk of costly damage, and monitor and detect abnormal activities in real time.
- To adapt to the changing nature of users and businesses, and the constantly growing numbers of attackers and methods they use.

Solution

Predica designed and implemented a solution based on Microsoft Advanced Threat Analytics to identify, prioritize and investigate cyber-attacks happening inside the organization.

- It helps to identify breaches and threats using behavioral analysis and pieces of machine learning.
- After detecting suspicious activities, known security issues and malicious attacks in near real-time, the tool provides clear, functional, actionable information on a simple attack timeline.
- The solution allowed the client to prioritize and plan for the next steps, making it possible to focus only on important events.