Bezema increases information security

Reference study IBM Security Network Intrusion Prevention System – GX Series

The customer: Bezema AG, Montlingen

Bezema AG in Montlingen is a company in the globally active CHT Group. It supplies high quality and innovative products to customers in the textile finishing industry, textile care sector and construction chemical industry. Bezema AG has its headquarters in the Swiss Rheintal, and thereby lies in the border triangle Switzerland – Austria – Germany, the traditional location for the textile industry with an international reputation.

„By deploying the IBM security appliance, we can react immediately to attacks and malware, minimize damage and further improve information security in our company“

Peter Bossart, head of ICT Bezema AG

Highlights

- **Simple to integrate:** The IPS solution works technically like a conventional bridge, and Bezema was able to put it into operation without any difficulty. No changes to the existing netork structure were necessary.
- **Rapid implementation:** The entire solution was installed onsite with an effort of 1 day. The fine-tuning of the IPS solution was then carried our remotely via a secure VPN connection.
- **High availability:** Thanks to the fail-open functionality integrated into GX series, the availability of the server infrastructure is guaranteed, even if there is an outage of the hardware used.
- **Reporting:** Management continuously receives reports about the technical state of the security and any incidents, and is therefore in a position to recognize the value of the investment.

The challenge

Due to a malware attack in 2009, the ICT department asked itself how it could regain control of the situation and how it could arm itself against future attacks.
As in many other companies, conventional security components such as a firewall and desktop-based anti-virus were used at that time.
What made the situation more complicated at Bezema was that in addition to the permanent network, two other external networks had to be connected, and the company employed a multitude of field workers, who travel the world with their laptops.
Some effort and thought are required to efficiently protect such an infrastructure. At Bezema, people were quickly in agreement that it was not just about fighting the malware, but that more importantly, effective precautions needed to be taken to prevent such attacks in the future.

The solution

Bezema decided on the installation of an Intrusion Prevention System (IPS) by the IBM Business Partner Mips Computer AG.

A modern IPS can already detect attacks on systems at the protocol level and, in contrast to a firewall, understands the languages used in prevalent protocols (http, ftp, SMTP etc.). For example, if an attacker attempts to find out a password using brute force attacks, IPS recognizes the attack, raises the alarm and blocks the gatecrasher.

Such an IPS was installed on the perimeter at Bezema, where it checks the entire data traffic between the permanent network, the external networks and the Internet.

An IPS is not a static system. The latest findings of the IBM X-Force research teams constantly flow into the solution and thereby continually raise the security level. An IPS system needs to be maintained in order to function optimally.

The solution has been used at Bezema for about a year now, and several attacks through malware have been discovered on time and rebuffed.

The advantages of the IPS solution Proventia GX

- **Recognizes and understands more than 200 protocols:** the current version of the protocol analysis modules understands more than 200 protocols thanks to the IBM X-Force technology, and can therefore analyze the entire traffic and react appropriately.
- **Preventive protection through IBM Virtual Patch technology:** it protects vulnerable systems by preventing attacks on weak points of exposed systems. In this way, valuable time for the testing and rollout of security updates and patches is gained, through which the weaknesses are eliminated.
- **Web Application Security:** protects Web applications such as Webserver, Webshops and Web 2.0 applications and offers the security level of a Web application firewall.
- **Transparent and invisible to attackers:** as the **s**ecurity appliance is resident on Layer 2 of the ISO/OSI model, it can be integrated into any existing network infrastructure without difficulty.
- **Performance:** different models allow an analysis of the data stream up to a capacity of 8 Gbps, with a latency of less than 200 microseconds.
- **Central management and reporting:** the IBM security solutions can be centrally controlled by the equally centrally available „Site Protector“ management console. A high-performance reporting tool is also integrated.

Contact:

IBM Switzerland
Markus Böck
Vulkanstrasse 106
PO Box
8010 Zurich

Mips Computer AG
Roger Schmid
Oberdorfstrasse 13
PO Box
6340 Baar

®yes

Brand names from other companies/manufacturers will be accredited. Contract conditions and prices can be obtained from the IBM offices and the IBM Business Partners. The product information reflects the current stand. The subject and scope of the services are defined exclusively according to the relevant contracts.

The publication on hand is for general information only.