Bezema erhöht die Informationssicherheit

Referenzstudie IBM Security Network Intrusion Prevention System der GX-Serie

Der Kunde: Bezema AG, Montlingen

Die Bezema AG in Montlingen ist ein Unternehmen der weltweit tätigen CHT-Gruppe. Sie beliefert Kunden aus der Textilveredelungsindustrie, Textilpflege und Bauchemie mit hochwertigen und innovativen Produkten. Die Bezema AG hat ihren Sitz im Schweizer Rheintal und liegt somit im Dreiländereck Schweiz – Österreich – Deutschland, dem traditionellen Textil-Standort mit Weltruf.

„Durch den Einsatz der IBM Security Appliance können wir umgehend auf Attacken und Schädlinge reagieren, den Schaden minimieren und die Informationssicherheit in unserem Unternehmen weiter verbessern“

Peter Bossart, Leiter ICT Bezema AG

Highlights

- **Einfach integrierbar:** Die IPS-Lösung arbeitet technisch wie eine herkömmliche Bridge und konnte bei Bezema mühelos in Betrieb genommen werden. An der bestehenden Netzwerkstruktur waren keinerlei Änderungen erforderlich.

- **Schnelle Implementierung:** Die gesamte Lösung konnte mit einem Arbeitsaufwand von 1 Tag vor Ort installiert werden. Das Fine-Tuning der IPS-Lösung erfolgte danach remote via gesicherte VPN-Verbindung.

- **Hohe Verfügbarkeit:** Dank der Fail-Open-Funktionalität, die in die GX-Serie integriert ist, wird die Verfügbarkeit der Serverinfrastruktur selbst bei einem Ausfall der eingesetzten Hardware gewährleistet.

- **Reporting:** Das Management erhält laufend Reports über den technischen Stand der Sicherheit und allfällige Vorfälle und ist so in der Lage, den Wert der getätigten Investition zu erkennen.

Die Herausforderung

Aufgrund einer Schädlingsattacke in 2009 stellte sich die ICT-Abteilung die Frage, wie die Situation wieder in den Griff zu bekommen sei und wie sie sich für zukünftige Angriffe wappnen solle.
Wie bei vielen anderen Unternehmen standen damals herkömmliche Sicherheitskomponenten wie Firewall und desktopbasierter Virenschutz im Einsatz.
Erschwerend kam bei Bezema hinzu, dass neben dem Stamm-Netzwerk noch zwei weitere, externe Netzwerke eingebunden werden mussten und dass das Unternehmen eine Vielzahl von Aussendienstmitarbeitern beschäftigt, die mit Laptops rund um die Welt unterwegs sind.
Um eine solche Infrastruktur effizient zu schützen, bedarf es einiger Anstrengungen und Überlegungen. Bei Bezema war man sich schnell einig, dass es nicht nur galt, die Schädlinge zu bekämpfen, sondern vielmehr Vorkehrungen zu treffen, um solche Attacken zukünftig wirksam zu verhindern.

Die Lösung

Bezema entschied sich für die Installation eines Intrusion Prevention System (IPS) durch den IBM Business Partner Mips Computer AG.

Ein modernes IPS kann Angriffe auf Systeme bereits auf Protokollebene erkennen und versteht im Gegensatz zu einer Firewall die Sprache, die in den gängigen Protokollen verwendet wird (http, ftp, SMTP u.a.). Versucht beispielsweise ein Angreifer, mittels Brute-Force-Attacke ein Passwort herauszufinden, so erkennt IPS den Angriff, schlägt Alarm und blockt den Eindringling ab.

Bei Bezema wurde ein solches IPS am Perimeter installiert. Somit überprüft es den gesamten Datenverkehr zwischen dem Stamm-Netzwerk, den externen Netzwerken und dem Internet.

Ein IPS ist kein statisches System. Laufend fliessen die neuesten Erkenntnisse des X-Force Research Teams von IBM in die Lösung ein und erhöhen so das Sicherheitsniveau kontinuierlich. Ein IPS-System muss gepflegt werden, um optimal funktionieren zu können.

Die Lösung steht bei Bezema nun seit rund einem Jahr im Einsatz und es wurden mehrere Angriffe durch Schädlinge rechtzeitig entdeckt und abgewehrt.

Die Vorteile der IPS Lösung Proventia GX

- **Erkennt und versteht mehr als 200 Protokolle:** Die aktuelle Version des Protocol Analysis Modules versteht dank der IBM X-Force Technologie mehr als 200 Protokolle und kann so den gesamten Verkehr über diese analysieren und entsprechend reagieren.
- **Präventiver Schutz durch die IBM Virtual Patch Technologie:** Sie schützt gefährdete Systeme, indem sie Angriffe auf Schwachstellen exponierter Systeme verhindert. So wird wertvolle Zeit für das Testen und den Rollout von Sicherheits-Updates und Patches gewonnen, mit denen die Schwachstellen behoben werden.
- **Web Application Security:** Schützt Web-Applikationen wie Webserver, Webshops und Web-2.0-Anwendungen und bietet das Sicherheitsniveau einer Web Application Firewall.
- **Transparent und für Angreifer unsichtbar:** Da die Security Appliance auf dem Layer 2 des ISO/OSI-Modells angesiedelt ist, kann sie mühelos in jede bestehende Netzwerkinfrastruktur integriert werden.
- **Performance:** Unterschiedliche Modelle erlauben eine Analyse des Datenstroms bis zu einem Durchsatz von 8 Gbps, mit einer Latenzzeit von weniger als 200 Mikrosekunden.
- **Zentrales Management und Reporting:** Mit der ebenfalls verfügbaren zentralen Managementkonsole „Site Protector“ lassen sich die IBM-Sicherheitslösungen zentral steuern. Zusätzlich ist ein leistungsstarkes Reporting-Tool integriert.

Kontakt:

IBM Schweiz
Markus Böck
Vulkanstrasse 106
Postfach
8010 Zürich

Mips Computer AG
Roger Schmid
Oberdorfstrasse 13
Postfach
6340 Baar