POWER GENERATOR KOSPO SAFEGUARDS ITS CRITICAL INFRASTRUCTURE WITH MAXPATROL™

THE CHALLENGE

Bring vulnerability and compliance management in-house; replace annual security assessments by external consultants with an automated solution covering the entire IS infrastructure; monitor compliance of all systems with Korea's MSIP standards out-of-the-box

Like all organizations involved in maintaining South Korea's critical infrastructure, energy generator KOSPO must comply with information security standards set by the government, including the Ministry of Science, ICT, and Future Planning (MSIP). In the past, the power firm met this obligation by employing government-approved consultants to perform annual assessments of IT systems at its many electricity plants and administrative offices.

Although these manual assessments satisfied the regulators, KOSPO knew that it was not an ideal approach to managing risk. "One security assessment per year was not enough to cover our rapidly changing IT infrastructure," said a spokesman for KOSPO's Information Security Strategy Department. "We wanted to be able to check our own compliance regularly so we could address any issues long before our annual audit. A reduction in consultancy costs was also desirable."

The quality of data available to KOSPO on its risk levels was also poor. "We were using a number of separate tools to check different parts of our infrastructure for vulnerabilities. This was an inefficient process and the tools were rarely updated by the vendors, so they did not protect us against the latest attacks. When you are dealing with critical infrastructure, this kind of risk is unacceptable. We needed a single solution that was regularly updated and could assess all our IT systems for both vulnerabilities and compliance."

Maintaining data security is a key priority for KOSPO, leading the organization to only consider locally-hosted solutions that would keep all confidential information on-site.

THE SOLUTION

MaxPatrol™ vulnerability and compliance management

The MaxPatrol™ vulnerability and compliance management solution is hosted at KOSPO's headquarters in Busan, around 250 miles South East of Seoul. It is used to scan all IT devices within the KOSPO infrastructure. KOSPO staff can now conduct on-demand, automated scans of the organization's various network devices as well as servers running Windows, Linux, and UNIX operating systems.

Checks for South Korea's MSIP regulations are included as standard in the MaxPatrol™ compliance mode. This allows KOSPO to rapidly check their progress towards annual certification as well as to assess compliance with other international guidelines such as ISO 27001.

The MaxPatrol™ audit mode gives a full picture of KOSPO's IT infrastructure, including installed software; version numbers and the updates/patches present on each IP. Meanwhile pentest mode identifies any vulnerabilities and misconfigurations using the renowned Positive Technologies knowledge base. The MaxPatrol™ server in Busan receives regular, automatic updates as the Positive Technologies research team identifies new threats.

The MaxPatrol™ agentless technology ensured a rapid roll-out for the solution across multiple power generation plants and administrative sites. KOSPO's Information Security Strategy Department was able to carry out automated vulnerability and compliance procedures within a month of the project commencement in December 2014.

COMPANY PROFILE

+ **Industry:**
  Energy Generation
+ **Operations:**
  Nine power plants including oil, gas and wind-powered sites. Additional plants planned in Korea, Sri Lanka, Chile, and Jordan
+ **Market Share:**
  11% of South Korea's total power generation capacity
+ **Ownership:**
  A subsidiary of South Korea's largest utility company, KEPCO

KOSPO

HIGHLIGHTS

- **Delivered Autonomous Compliance Management** by empowering KOSPO to conduct its own checks against government standards and international guidelines such as ISO 27001
- **Reduced Security Costs** by eliminating reliance on third party security consultants
- **Enhanced Visibility of Threats** by consolidating vulnerability management in a single solution that is regularly updated to detect new threats
- **Safeguarded Confidential Data** with a solution that keeps all scan information on customer's site

THE BENEFITS

In-house control of MSIP compliance, enhanced visibility of risk levels, lower consultancy costs

"With MaxPatrol™, we have taken control of our security posture," said the KOSPO spokesman. "Instead of a single, annual security assessment by external consultants, we can now conduct checks ourselves whenever we want. We have much more visibility of our risk as well as reduced costs for hiring consultants. The regular updates to MaxPatrol™ also mean we can check for exposure to new worldwide vulnerabilities on the scale of Heartbleed or Shellshock as soon as they are uncovered."

Combining all vulnerability and compliance management tasks into a single solution has improved efficiency within the Information Security Strategy Department. "We can now prepare more effectively for our government audits. We are also able to rapidly check the configuration of all new servers before they go into production," added the spokesman.

With a mass of results produced by the MaxPatrol™ detailed scans, it was important that KOSPO was able to control and easily interpret the data. "Having all our security information stored within our own data center gives us confidence that our private records will not be compromised," said the spokesman. "The flexible reporting features in MaxPatrol™ allow us to generate many different reports with appropriate levels of detail for each of the management levels within KOSPO and our parent company as well as for the government auditors."

Having seen the benefits of MaxPatrol™ for its IT systems, KOSPO is now looking to extend its use of the solution to manage vulnerabilities and compliance for its SAP and SCADA systems and virtualization platforms.

About Positive Technologies

Positive Technologies is a leading provider of vulnerability assessment, compliance management, and threat analysis solutions to more than 1,000 global enterprise clients. Our solutions work seamlessly across your entire business: securing applications in development; assessing your network and application vulnerabilities; assuring compliance with regulatory requirements; and blocking real-time attacks. Our commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on SCADA, banking, telecom, web application, and ERP security, and distinction as the #1 fastest growing Security and Vulnerability Management firm in 2012, as shown in an IDC report*. To learn more about Positive Technologies please visit ptsecurity.com.

*Source: IDC Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares, doc #242465, August 2013. Based on year-over-year revenue growth in 2012 for vendors with revenues of $20M+.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com