Q&A

HYOGO PREFECTURE, A PROMOTER OF "SMART MUNICIPALITIES", ADOPTS TENABLE.AD TO ENHANCE ITS ACTIVE DIRECTORY SECURITY

Business Case:

Hyogo Prefecture has strengthened its information security measures by moving to the β′ model, as defined in the new guidelines on information security policy for local government. As part of this effort, Hyogo Prefecture adopted Tenable.ad to strengthen its Active Directory security measures. We interviewed Kenichiro Tanaka, who is responsible for managing the system operations at Hyogo Prefecture.

CASE STUDY: HYOGO

Company: Hyogo Prefecture, Japan

Official Website: https://web.pref.hyogo.lg.jp/fl/

Number of Households: 2,430,402 (as of October 1, 2022)

Population: 5,403,823 (as of October 1, 2022)

Impact of Tenable deployment:

- Can visualize dormant accounts, etc. and delete unnecessary accounts
- Can identify and mitigate vulnerabilities in Active Directory configuration, etc.
- Significantly improved the security of the Hyogo Prefecture Information Security Cloud

Solution

tenable.ad

Interviewee:

Mr. Kenichiro Tanaka - Unit Chief
Hyogo Prefecture, Department of Planning,
Digital Transformation Section, System Planning Unit

Hyogo Prefecture is implementing multiple measures as part of becoming a Smart Municipality

Interviewer: Please tell us about the features of Hyogo Prefecture's municipal systems and security measures.

Mr. Tanaka: Hyogo Prefecture is working on its Smart Hyogo Strategy as a "smart municipality", the aim of which is to improve the accessibility and quality of administrative services for prefectural residents through the use of information technology. We've also been developing Telework Hyogo since November 2020, with the intention of transforming work styles in the post-COVID-19 era.

Telework Hyogo is a new telecommuting system infrastructure not just for the prefectural government itself, but also for city halls, town halls, schools, and small to medium-sized businesses within the prefecture. By installing a dedicated connection application on both work and home PCs, users can easily and safely access their workplace PCs from home.

Currently, more than 62,000 people are using this application, which will be free of charge until December 2023. We have received positive feedback from users, who are saying, "It doesn't take long to set up, and I can work just as if I was at work".

Interviewer: Please tell us about your department and the nature of your work.

Mr. Tanaka: I belong to the Digital Transformation Division. The department deals with digital transformation but with a particular focus on management of internal systems, and has 29 staff. We primarily operate the prefectural government WAN (Wide Area Network) to improve administrative services, and establish a secure and efficient administrative system.

In addition, we maintain and operate the Hyogo Information Highway, which is an efficient network infrastructure for networks in various administrative fields, such as the prefectural government WAN and the educational information network connecting prefectural schools. We are also promoting the use of open and shared infrastructure systems.

Furthermore, we're developing information security policies to strengthen the prefectural systems, through efforts such as operating the Hyogo Prefecture Information Security Cloud, and transitioning to the ß' model as defined in the new guidelines on information security policy for local government, recommended by the Ministry of Internal Affairs and Communications. Within this scope, I manage the Telework Hyogo operations.

Visualizing the vulnerabilities in Active Directory was a challenge

Interviewer: Please tell us about the challenges you were facing before you adopted Tenable.ad.

Mr. Tanaka: For Hyogo Prefecture's prefectural network, we've been working on transitioning administrative systems and staff computers, except for the systems used for My Number operations (My Number is a unique identifying number allocated to citizens for Social Security and Tax purposes), to properly secured Internet-

based systems. This corresponds to the transition to ß' model described in the new guidelines on information security policies for local government. This transition was carried out in FY2021.

The Hyogo Prefecture Information Security Cloud is the central point from where we manage user accounts and client terminals through the use of Active Directory (hereinafter referred to as "AD"). Centralized management by AD is extremely efficient, and helps reduce the load of managing user terminals.

However, AD with inadequate security countermeasures is an easy target for bad actors looking for a stepping stone to privilege escalation, or looking to explore other system areas by taking advantage of known vulnerabilities and misconfiguration.

Hyogo Prefecture has been applying security patches and other measures, but there had never been a tool to visualize the vulnerabilities in AD itself, and we felt that this was an issue.

The prefectural government adopted the highly reliable Tenable.ad based on its experience with Nessus, another Tenable product

Interviewer: You chose to adopt Tenable.ad to visualize vulnerabilities in AD, but please tell us what brought you to this decision.

Mr. Tanaka: We were looking for a security product for AD, as we'd been seeing many cases of cyber attacks targeting AD. Hyogo Prefecture had already been using Nessus for security vulnerability checks for some time, and we were satisfied with its performance, functionality, and ease of use. So, we felt that going for Tenable.ad from the same company would be a more reliable and safer choice than going for a product from another company. We also found many beneficial features in Tenable.ad. It can identify vulnerabilities in AD and can detect new attack vectors, has real-time detection features, and allows visualization of the risks present in AD.

Interviewer: Please tell us about any problems you faced with its adoption.

Mr. Tanaka: We began considering Tenable.ad around August 2021 and started using it at the end of the fiscal year. It's been a little over six months since we adopted it. Thanks to Tenable's support, the adoption itself was completed at a rapid pace. It took less than a month, which was extremely helpful.

Adoption of Tenable.ad resulted in a significant reduction of vulnerabilities in Active Directory

Interviewer: Please tell us about the impact of adopting Tenable.ad.

Mr. Tanaka: First of all, it was a major relief that we were able to delete dormant accounts, which we had been concerned about as a vulnerability for some time. By utilizing Tenable.ad to identify unused accounts and by referring to other logs and histories, we were able to delete a significant number of unnecessary objects from AD. These were primarily dormant accounts of staff members who had retired or transferred.

In addition, Tenable.ad also has a feature for calculating compliance scores. This feature keeps track of the status of dormant accounts and password policy compliance, as well as of account trust relationships, inappropriate configurations, and changes in AD, and quantifies the risk status of AD based on each of these observed points.

Our compliance score has improved dramatically. Risk items can be identified individually, and recommended remediation can be viewed for each one. By addressing these issues, we improved our score significantly. We feel that this has contributed greatly to improving the security of AD.

Compliance scores can also be generated as audit reports, and this allows us to periodically generate reports to monitor the scores on an ongoing basis. For the Hyogo Prefecture Information Security Cloud in particular, ID management is extremely important, and we feel that Tenable.ad has strengthened our ID management system.

The prefecture intends to further improve the accessibility and security of its services

Interviewer: Please tell us if you have any thoughts on future security measures, beyond the scope of AD.

Mr. Tanaka: Cyber attacks are evolving rapidly, becoming more sophisticated and complex every year. And so, security measures must be updated accordingly. In Hyogo Prefecture, we updated the Hyogo Prefecture Information Security Cloud in FY 2021 to enhance its security and cloud features.

Specifically, the enhanced security features are protection by WAF (Web Application Firewall) against attacks on our web apps, website access distribution by CDN (Content Delivery Network), email security enhancement by targeted attack countermeasures, and system security enhancement by behavior detection.

We intend to continue to use the Hyogo Information Security Cloud to improve user experience and develop information security measures.