CASE STUDY

PUBLIC SERVICES. CRITICAL DATABASE. CYCLICAL ATTACKS.

Public Sector Organisation

OVERVIEW

"This is a solution that you can't live without. If we hadn't installed Tenable.ad, we would never have known about these attacks."

Enterprise Architect
Large Local Authority, UK

BUSINESS NEEDS

Organisation: Large local authority, UK

Employees: 17,000

Industry: Public services

Challenges

- Increasing public sector cyberattacks
- Improve exposure visibility around Active Directory
- Monitor and secure Active Directory on an ongoing basis

Solution

tenable.ad

Results:

- Efficient installation and configuration of Tenable.ad
- Alerted to Brute Force attacks in real time
- Alerted to Golden Ticket attacks in real time
- Targeted accounts disabled and attacks shut down swiftly
- Able to trace attacks to a single server, which was taken offline
- Prevented further damage as well as huge fines
- Real-time monitoring

CHALLENGE

Public sector Organisation: Serving citizens

One of the larger local authorities in the UK provides a full range of public services to its population. Security is paramount for the organisation, which processes personal data for citizens, including children and vulnerable adults, as well as sensitive commercial, third-party, and National Health Service (NHS) data. As a government facility, it's subject to strict data security regulations and oversight. With the recent rise in cyberattacks targeting government websites and services, the organisation was looking to increase security for its Active Directory (AD) to prevent domain control from falling into the wrong hands.

GAINING VISIBILITY INTO AD SECURITY DUE TO RISING ATTACKS + REGULATION REQUIREMENTS

The local authority uses a single forest AD structure with parent-child domains to control access to its internal servers and external facing services. In addition to compliance certification and data sharing agreements, the organisation is subject to oversight by numerous regulatory bodies including the Public Services Network (PSN), Office for Standards in Education, Children's Services and Skills (Offsted), the Department of Education, and the Information Commissioner's Office (ICO)—which issues hefty fines for any failure to report a data breach within a strict timeframe. It also has to comply with GDPR, PCI DSS, and the DSP toolkit for NHS data. Plus, it's just one branch away from the central UK government, making security all the more critical.

The organisation's enterprise architect team is made up of a security team, responsible for everything from writing policies to managing cyberattacks, and an operations team, which handles day-day-day AD administration and vulnerability management.

Knowing there was a recent rise in cyberattacks against local government branches, the security team was looking to secure the AD specifically and address these critical priorities:

- **Identify** existing vulnerability indicators early and take proactive steps to remediate.
- **Maintain** security by gaining visibility into AD architecture.
- **Receive** real-time alerts when under attack.

The team needed a single solution that would enable them to monitor AD security on an ongoing basis, indicating flaws that appear, so they can be remediated before they impact the network.

SOLUTION

Real-time analytics and visibility enable immediate response

The organisation already had Tenable in place to help with its vulnerability management efforts. To secure AD, which is often the target of criminal attacks seeking valuable privileges and data, it added Tenable.ad to its security stack in later summer of 2021. As it turns out, the team deployed the solution just in time.

A national bank holiday had the organisation's offices scheduled to be closed for a long weekend. The team implemented Tenable.ad on its servers on a Wednesday with all alerts enabled. Friday morning, they discovered multiple Brute Force attacks on administrator accounts taking place including one Golden Ticket attack, which was soon followed by many others. Over the next three days, Brute Force and Golden Ticket attacks continued to occur in a cycle.

According to the organisation's enterprise architect, "If we didn't have Tenable.ad, we would never have known. We would have come back from the long bank holiday weekend and been locked out of our network. We were very lucky to get Tenable.ad in place."

RESULTS

Mitigating damage and identifying the source

With Tenable.ad alerting them to the attacks in real-time, the team was able to immediately disable the targeted accounts. The Enterprise Architect explains, "We were able to take charge of what was happening very quickly." The speed of response was critical to preventing further damage, including compromised access and data leaks.

Using the detailed information that Tenable.ad alerts provided regarding the attacks, the enterprise team was able to immediately specify which accounts needed to be disabled. "Tenable.ad told us very quickly who they were and we disabled those accounts very, very quickly," says the Enterprise Architect.

But every time they shut down one attack, another was initiated. They realized this was not a singular attack. Someone was on their network exploiting these accounts. In addition to disabling accounts, the team also started physically removing devices from the network—literally pulling the plugs. That evening they reset the password of the Kerberos ticketing agent to prevent further Golden Ticket attacks. However, the attacks continued the next day. And with the help of Tenable.ad, the team continue to shut them down.

By leveraging Tenable.ad's real time analytics and visibility, they played a high stakes game of cat and mouse over the next two days, disabling IT network management accounts, pulling servers from the network, and removing data center servers from the cluster. Even after performing a second Kerberos ticketing agent password reset, the attacks continued. But by Sunday, they were able to verify that all infected servers were taken offline, which was proven to be correct as the attacks stopped.

About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organisations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies.

Learn more at www.tenable.com.

CONCLUSION

Greater visibility, proactive response, and a better security posture

Tenable.ad was instrumental in negating cyclical Brute Force and Golden Ticket attacks that went on for days. Had the organisation not installed Tenable.ad, the attacks would have gone unnoticed. With Tenable.ad in place, the attacks were detected and any potential security issues as well as resulting fines were successfully avoided.

The Enterprise Architect says, "The visibility we gained from Tenable.ad not only allowed us to prevent a data leak and the damage that would have done to our reputation, it's brought security back to the forefront." Following on their success with Tenable.ad, the organisation introduced Tenable.io as a vulnerability management and reporting solution. After seeing what happened here, multiple other local authorities across the country also invested in Tenable.ad and Tenable.io. It's helped them mitigate being in the same situation as well.

Learn more at tenable.com/products/tenable-ad or start a conversation: marketing@tenable.com

Learn more at tenable.com/products/tenable-ad or start a conversation: marketing@tenable.com