THE CITY OF KEIZER ENHANCES CYBERSECURITY BY ELIMINATING COMPROMISED PASSWORDS

The City of Keizer is a beautiful community in the Willamette Valley of Oregon. The city offers an ideal environment, delivering a range of services to citizens, from parks and public works to police protection.

However, even from its earliest days, there have been hazards to overcome. As a settlement in the 1800s, floods forced the community to rebuild on higher ground and eventually add dams to control the river's flow. Today, the hazards come from cybercriminals. In 2020, the City of Keizer was targeted with ransomware attacks that jeopardized sensitive data and essential services. To defend the community, the city has introduced new types of protection and controls. Bill Hopkins is responsible for Information Technology for the City of Keizer and brought in Enzoic to support his initiative.

What prompted the search for a password hardening solution?

After the ransomware incident, the city conducted a forensic investigation to identify our vulnerabilities and ways to improve our defenses against future attacks. We determined that passwords were a significant problem.

Cybercriminals can perform simple attacks using email addresses and passwords found on the web. We were sure many of our users' email addresses and their domain passwords were vulnerable.

Unsafe passwords put us at risk of further ransomware attacks and other forms of hacking and account takeover.

What type of cybersecurity solutions did you consider?

Since the attack, we've applied many new technical and procedural security improvements, but we knew hardening passwords needed to be among our first priorities. We couldn't allow our users' passwords to be found floating on the Internet. We needed to enhance our password policies in Active Directory.

We also knew passwords could start out safe but could become unsafe if they appeared in a later data breach. It's tough to get employees to create good passwords, and password reuse creates additional risks. Password reuse basically expands the perimeter we need to be concerned about. We wanted a way to keep scanning our Active Directory environment against credentials exposed in new data breaches.

There are a few solutions out for password blacklists, but none were as comprehensive. Enzoic offered a simple solution to address a clearly defined problem at a reasonable price. For us, Enzoic was really the only game out there.

THE CITY OF KEIZER ENHANCES CYBERSECURITY BY ELIMINATING COMPROMISED PASSWORDS

How does hardening passwords fit with MFA?

Authentication security is essential, so we did also add 2FA for our users' accounts. But having gone through what we did with ransomware, hardening the password layer was still essential. So, we look at 2FA as adding an extra layer of protection. It wouldn't make sense to rely on a multi-factor approach while knowing that our passwords weren't secure.

Our password layer is not going away anytime soon. Until we eliminate passwords altogether, we need to make sure they are kept secure.

How complicated was the Enzoic deployment?

The deployment was pretty much seamless. It's a simple installation on our domain controllers and a wizard-based configuration.

We had an interaction with Enzoic support and found them very responsive and knowledgeable.

We used the ability to select Active Directory accounts by Organizational Unit or Group in Active Directory. This gave us the flexibility to tailor coverage to specific configurations we needed. We also particularly liked Enzoic's continuous monitoring capabilities. This provided the ability to detect when a password becomes compromised later.

Our next step will be to deploy Enzoic's Windows Client to give users information about the password policy and feedback when a password doesn't meet that policy.

Has the project been successful?

Our project goal was to keep any common, compromised, or easy to guess passwords out of our environment. It was very easy to do this with Enzoic since new passwords are evaluated in real-time.

We also identified and automatically disabled several accounts whose credentials showed up in new data breaches during our first few months.

We know data breaches happen every day, so having a solution that keeps current is critical. And the fact that the whole continuous audit and resolution happens without manual involvement was significant given our resource limitations.